Virginia Information Technologies Agency

Commonwealth Information Security Officers Advisory Group (ISOAG) Meeting

October 2, 2013

Virginia Information Technologies Agency

ISOAG October 2013 Agenda

I.	Welcome & Opening Remarks	Mike Watson, VITA
II.	Enterprise Password Insecurity	Hank Leininger, KoreLogic
III.	Counterfeiting	SA Jonathan Schanke, FBI
IV.	Data Point Deep Dive	Mike Watson, VITA
V.	EOL Software: Considerations & Controls	Bob Baskette, VITA
VI.	2013 Penetration Test	Bob Baskette, VITA
VII.	Upcoming Events	Mike Watson, VITA
VIII.	Partnership Update	Bob Baskette, VITA Michael Clark, NG

KoreLogic SECURITY

Enterprise Password Insecurity

Hank Leininger
KoreLogic

https://www.korelogic.com/

Agenda

- **Background**
- Anatomy of Password Cracking
- Public Password Disclosures
- Enterprise Password Strength Policies
- New Directions In Password Cracking

KoreLogic SECURITY

My Background

Played defense as a sysadmin / security admin since the mid 90's.

Had to learn how to think like the bad guys.

Decided that attackers had more fun.

Have been doing security consulting since 2000; co-founded KoreLogic in 2004.

We created the Crack Me If You Can contest at DEFCON; 2013 was its 4th year running.

I also run the MARC mailing list archive site: http://marc.info/

Your Backgrounds

How many of the folks here use password cracking tools?

How many of your organizations do not rely on passwords—use 2-factor authentication like SecureID, SSH keys, SmartCards, x509 Client Certificiates, etc?

Agenda

- Background
- **Anatomy of Password Cracking**
- Public Password Disclosures
- Enterprise Password Strength Policies
- New Directions In Password Cracking

KoreLogic SECURITY

Anatomy of Password Cracking

What is password cracking anyway?

If you know this one, now's a good time to check your email, but I'll review just in case.

Anatomy of Password Cracking – Online Attack vs Offline Attack

“Online” password-cracking typically means connecting to a target server over and over, and attempting to log in with guessed username & password pairs. This is noisy (generates logs), slow (relatively speaking), and likely to lock users out.

Usually, people just refer to this as login brute-forcing/guessing. “Password cracking” usually means “Offline” cracking, in which the attacker isn't connecting to the server over and over again.

Anatomy of Password Cracking – Offline Password Cracking

For a given system that encrypts users' passwords, the server converts a user's plaintext into a ciphertext using some specific encryption algorithm, and stores the ciphertext (/etc/shadow, Windows SAM, etc).

In an offline password-cracking attempt, an attacker has somehow gotten ahold of the encrypted hashes (the ciphertexts), and wants to determine the plaintexts.

Unless the cryptography is utterly, horribly broken (read: do-it-yourself), it's impossible with today's math to work backwards from a ciphertext to figure out what the original plaintext was.

- It's akin to being given the number 36, and not knowing if it was originally composed of 2x18, 3x12, 4x9, 6x6, or 108 / 3.

Anatomy of Password Cracking – What is it?

The attacker has to guess (or bruteforce) plaintexts; and keep trying the same encryption function the server uses:

```
for each candidate_plaintext
    result = encryption_function(candidate_plaintext)
    done if (result matches the ciphertext)
```

Exactly how the encryption function works typically depends on the underlying crypto algorithm (DES, MD5, SHA1) and how it is applied:

- MD5(plaintext)
- SHA1(salt . plaintext)
- MD5(MD5(MD5(MD5(plaintext))))

Anatomy of Password Cracking – Cracking tools

So at a high level, conventional password cracking tools need:

- To support the hashing algorithm of your target ciphertext, and hopefully be fast at it.
- To be able to generate candidate plaintexts to try.

Some tools are good at both of these; some really only one or the other.

Anatomy of Password Cracking – Cracking tools

So at a high level, conventional password cracking tools need:

- To support the hashing algorithm of your target ciphertext, and hopefully be fast at it.
- To be able to generate candidate plaintexts to try.

Some tools are good at both of these; some really only one or the other.

(Some are only really good at parting you from your money.)

Anatomy of Password Cracking – Cracking tools

Password cracking tools were traditionally CPU-based (because everything was):

- John the Ripper

  Support for lots of different hash types
  Runs on lots of different operating systems
  Fast by CPU-cracker standards
  Excellent at candidate-generation
  Free and open-source
- Hashcat

  Support for a good variety of hash types
  Runs on Windows, Linux, some other UNIXes
  Free, but closed-source
- Cain & Able

  Support for even more hash types
  Windows-only
  Free but closed-source
- L0phtCrack

  Pretty

Anatomy of Password Cracking – Cracking tools

In recent years GPU-based password crackers have been developed. Historically, GPU-crackers were fast, but dumb: they could only handle a few hash types (raw MD5, SHA1) and could only bruteforce (aaaaaaa, aaaaaab ...). But that has been changing:

- oclHashcat suite

  Limited algorithm support initially; more every month
  Unbelievably fast: 10x – 1000x as fast as a CPU, depending on the algorithm.
  Very smart at candidate generation
  Runs on Windows and Linux
  Free, closed-source

- Cryptohaze MultiForcer

  Limited algorithm support
  Very fast
  “Smart” brute forcer

Anatomy of Password Cracking – Cracking tools

Rainbow-table cracking tools work differently.

Rainbow tables are pre-generated data files (often big – terabytes and terabytes) built using a whole lot (months, years, or decades) of CPU time.

Those tables are then used as a partial lookup table when cracking a given ciphertext, resulting in a *huge* speedup (seconds or minutes instead of hours, days, or months).

Rainbow tables can be *really* effective in some circumstances. But for some they are useless; for others they work but are not the best tool for the job.

Agenda

- Background
- Anatomy of Password Cracking
- **Public Password Disclosures**
- Enterprise Password Strength Policies
- New Directions In Password Cracking

KoreLogic SECURITY

Public Password Disclosures

In recent years there have been many public disclosures of passwords and password hashes of large websites and other online communities:

- LinkedIn
- RockYou
- last.fm (multiple times)
- Evernote
- Various online games
- Twitter
- Virginia Tech
- Monster
- Sony, Sony, and Sony

Large scale breaches of PII (SSNs, etc) have pushed password disclosures out of the news somewhat.

Public Password Disclosures – What do they tell us?

There are two big lessons from all this exposed data (although neither is really new):

- As an IT professional: users, when given no password strength requirements, will choose really, really awful passwords.
  - 12345
  - 123456
  - password
  - qwerty
  - firstnamelastname
  - companyname
- As a human: expect to be betrayed by every company you interact with online. That way you'll be pleasantly surprised 50% of the time...

(But that isn't really our topic today.)

KoreLogic SECURITY

Agenda

- Background
- Anatomy of Password Cracking
- Public Password Disclosures
- **Enterprise Password Strength Policies**
- New Directions In Password Cracking

KoreLogic SECURITY

Enterprise Password Strength Policies

That's why enterprise environments always have password strength policies, right?

Minimum length, complexity rules (upper, lower, number, punctuation), and histories... those will keep us safe, right?

Enterprise Password Strength Policies

That's why enterprise environments always have password strength policies, right?

Minimum length, complexity rules (upper, lower, number, punctuation), and histories... those will keep us safe, right?

Wrong...

Enterprise Password Strength Policies – Easy for Users to Evade

A nice, strong-looking policy such as:

- Minimum 9 characters
- Upper & lowercase, numbers, punctuation

Enterprise Password Strength Policies – Easy for Users to Evade

A nice, strong-looking policy such as:

- Minimum 9 characters
- Upper & lowercase, numbers, punctuation

...Is perfectly happy to accept “P4ssword!”, J0hn.Sm1th”, etc.

Which—as we'll discuss later—are trivial to crack.

Enterprise Password Strength Policies – Easy for Users to Evade

Password expiration and password histories can also work against you.

How about we force users to change their passwords every 30 days, and they can't reuse for 18 months? Sound good?

Enterprise Password Strength Policies – Easy for Users to Evade

Password expiration and password histories can also work against you.

How about we force users to change their passwords every 30 days, and they can't reuse for 18 months? Sound good?

10% of them will currently have a password of “Oct2013!”, “Oct%2013”, or “Sept.2013!”

Even worse, once I know that, I can come back 12 months from now and guess it on the first try.

Enterprise Password Strength Policies – Driving Users Crazy

What's an IT person to do? Just keep requiring longer passwords? Where does that end? The DoD (for instance) requires 15-character passwords minimum.

Meanwhile, users are ready to mutiny because of what they perceive as draconian, over-the-top security measures.

We'll come back to this...

Assessment Experience

We do a lot of penetration tests of large and small enterprises.

These environments all enforce traditional password complexity.

In the face of that enforcement, users still herd in predictable ways, creating systemic weaknesses in enterprise passwords that attackers can leverage.

What We Typically See

- Users consistently choose the simplest passwords they can within the constraints they are given.
- Password Rotation leading to predictable, guessable behavior:
  - Common root words
  - Date-based passwords
  - Keyboard patterns
  - Location, Company, Industry-based dictionaries
  - Combining two dictionary words
  - Predictable number & special placement

Traditional Remediation Advice

There's no easy answer, but these help:

- Pro-actively crack your organization's passwords; force changes for the weakest.
- Include the “why” in password-strength user education
- Make secure password-storage a purchasing requirement—use salts, difficult algorithms, etc. (Unfortunately this would rule out MS Windows...)
- If users need to maintain lots of different sets of credentials, look for tools to facilitate that—GPG, KeePass, various commercial options.
- Push for stronger authentication methods
  - Public key (SSH authorized_keys, certificates – dare I say PKI?)
  - 2-factor using hardware tokens, SMS to mobile devices, etc.

Agenda

- Background
- Anatomy of Password Cracking
- Public Password Disclosures
- Enterprise Password Strength Policies
- New Directions In Password Cracking

KoreLogic SECURITY

New Directions In Password Cracking

- If I had given this presentation 10-15 years ago, it would have been almost identical up to this point, but would have ended here.
- In recent years, the computing power of GPU-based cracking has made “informed” or “targeted” brute-forcing practical.
- It turns out, users' passwords are also very vulnerable to this—again because of predictable human behavior.

“Dumb” Brute Force

- Exhaustive brute forcing of passwords—trying everything from aaaaaaaa, aaaaaaab, through ~~~~~~~~ is not generally practical.
- But, for very weak hash types, it is viable.
- For instance, suppose you built a machine with 3 AMD 7970 GPUs for about $2,000 total.
- That machine could try all possible 8-character NTLM passwords (the strongest hash type that Windows / Active Directory has to offer) in 48 hours.
- But, it would take 6+ months to try all 9-character NTLMs (or 10 days for 20 such machines). 10-character, about 50 years.

“Smart” Brute Force – Password Patterns

- Rather than testing all possible passwords, pick some specific patterns and try all passwords that fit that pattern.
- We'll use 'u' to represent "any uppercase latter", 'l' for "lowercase letter", 'd' for "digit", and 's' for "special" (punctuation). So, four possible character sets per password character.
- For an 8-character password, there are 4^8, or 65,536 possible patterns. For 9-character, 4^9, or 262,144 patterns.

“Smart” Brute Force – Password Patterns

- For instance, "P4ssword13!", "N0vember24@", "R3dskins99#" all use the same pattern: udlllllldds
- There are 5.6 x 10^21 possible 11-character passwords, which would take our cracking machine over 4,700 years to completely brute-force.
- However, there are only 265 trillion possible passwords that fit the pattern **`udlllllldds`** - we could brute-force all of those in just 11 hours!

KoreLogic SECURITY

Predictable Password Patterns

- So, if you can guess which patterns users have over-used, you can effectively bruteforce just those pattern spaces, and crack a disproportionate number of passwords.
- We analyzed the passwords we had cracked from several different enterprise assessments, looking for frequently used patterns.

Predictable Password Patterns

- So, if you can guess which patterns users have over-used, you can effectively bruteforce just those pattern spaces, and crack a disproportionate number of passwords.
- We analyzed the passwords we had cracked from several different enterprise assessments, looking for frequently used patterns.
- We found them...

Sample Organization #1: Fortune 100 Food & Beverage Company

- 263,356 of 263,888 logins cracked (including histories)
- 7,308 unique patterns found
- Most Popular Patterns:
  - 33,458 **`ullllldd`** (8 character)
  - 33,394 **`ullllllldd`** (9 character)
  - 27,898 **`ullldddd`**
  - 19,190 **`ullllllldd`**
  - 13,204 **`ullllddddd`**
- 99.9% of passwords meet their complexity requirements
  - They had recently increased their min length to 9.
  - History entries still had 8-char passwords.
  - Look at how similar the top 8-char patterns are to the top 9-char patterns!
- The top 100 patterns are used by a total of 85% of all users.

KoreLogic SECURITY

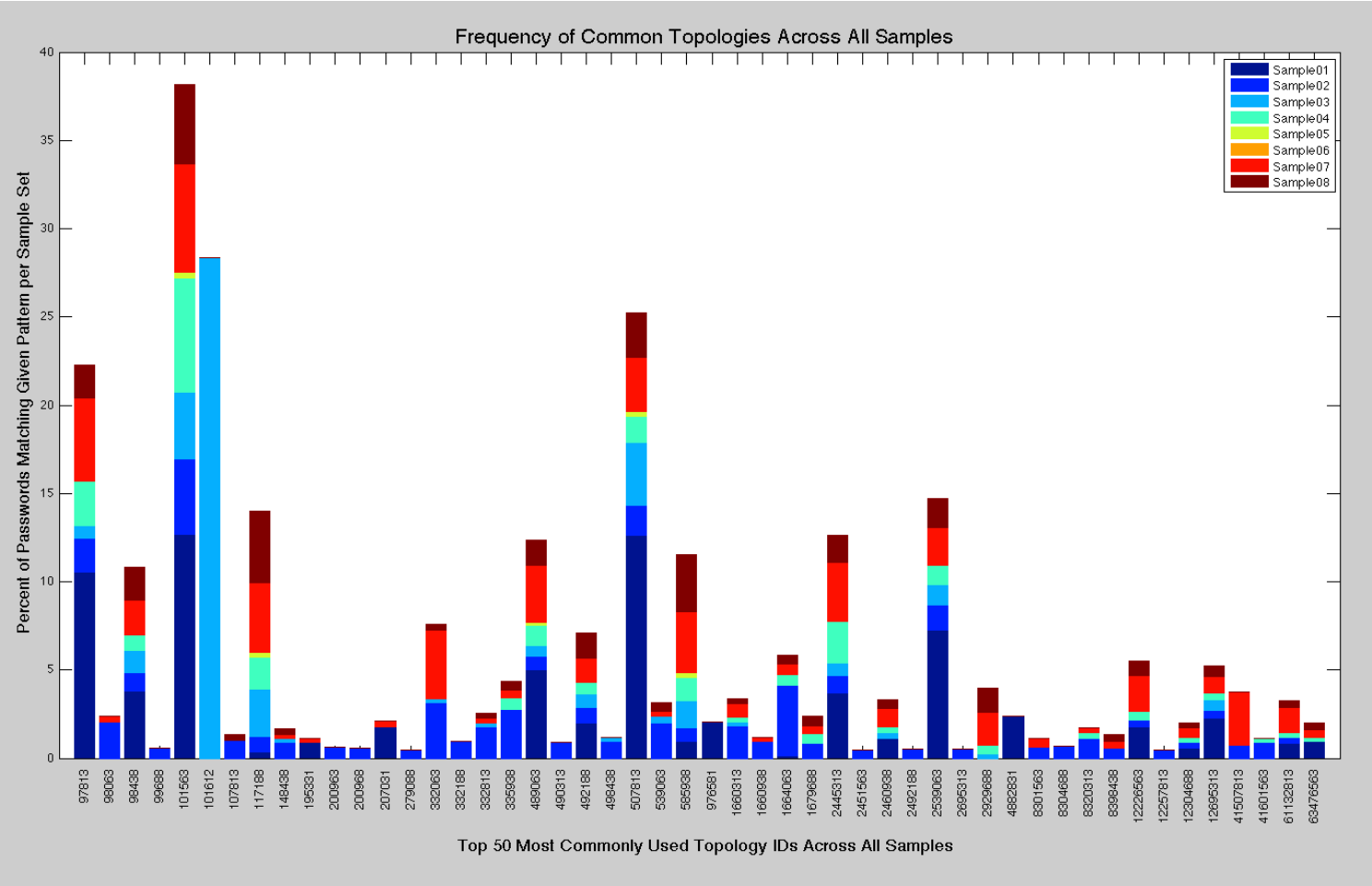
Sample Organization #2: Fortune 500 Financial Services Company

- 419,287 of 449,192 logins cracked (including histories)
- 14,266 unique patterns found
- Most Popular Patterns:
  - 19,200 **`ullllldd`** (8 character)
  - 17,914 **`ullllldds`** (9 character)
  - 14,025 **`ulldddds`**
  - 12,477 **`ullllds`**
  - 9,216 **`ullsdddd`**
- First 5 patterns crack 72,832 unique passwords (16% of all passwords)
- The top 100 patterns are used by a total of 62% of all users.

KoreLogic SECURITY

Similarities Across Organizations

We analyzed the patterns (password topologies) used by 8 different enterprises of 4,000 or more logins where we had cracked more than 90% of all password hashes. We found that they had popular topologies in common.



KoreLogic SECURITY

Defenses Need to Evolve

- We need to add a new dimension to password strength enforcement.
- Rules like minimum length, minimum character sets required, no dictionary words, etc are still needed.
- But we also need a way to prevent users from herding towards the same overused password patterns (topologies).

Defenses Need to Evolve

- As a first step, we could develop topology blacklists - patterns that we know will be overused if they are allowed, so don't allow them at all.
- Better would be something dynamic, that tracks topologies used by users, and prevents re-use when users go to change their passwords.
- And we need to figure out how not to be mobbed by angry users with pitchforks, when we activate such a protection mechanism.

Questions

Hank Leininger <hlein@korelogic.com>

KoreLogic SECURITY

Agenda

- Background
- Anatomy of Password Cracking
- Public Password Disclosures
- Enterprise Password Strength Policies
- New Directions In Password Cracking
- **Bonus: Crack Me If You Can**

KoreLogic SECURITY

Why a Password Cracking Contest?

We kept seeing the same password problems at different customer networks, kept having to give similar advice everywhere we went.

But we saw few people talking about this publicly, and new clients were always surprised when we pointed them out.

We wanted to change that.

DEFCON Crack Me If You Can 2010

KoreLogic sponsored a password cracking contest at DEFCON 18 in 2010, designed to highlight and get people talking openly about what we'd seen happening within corporations.

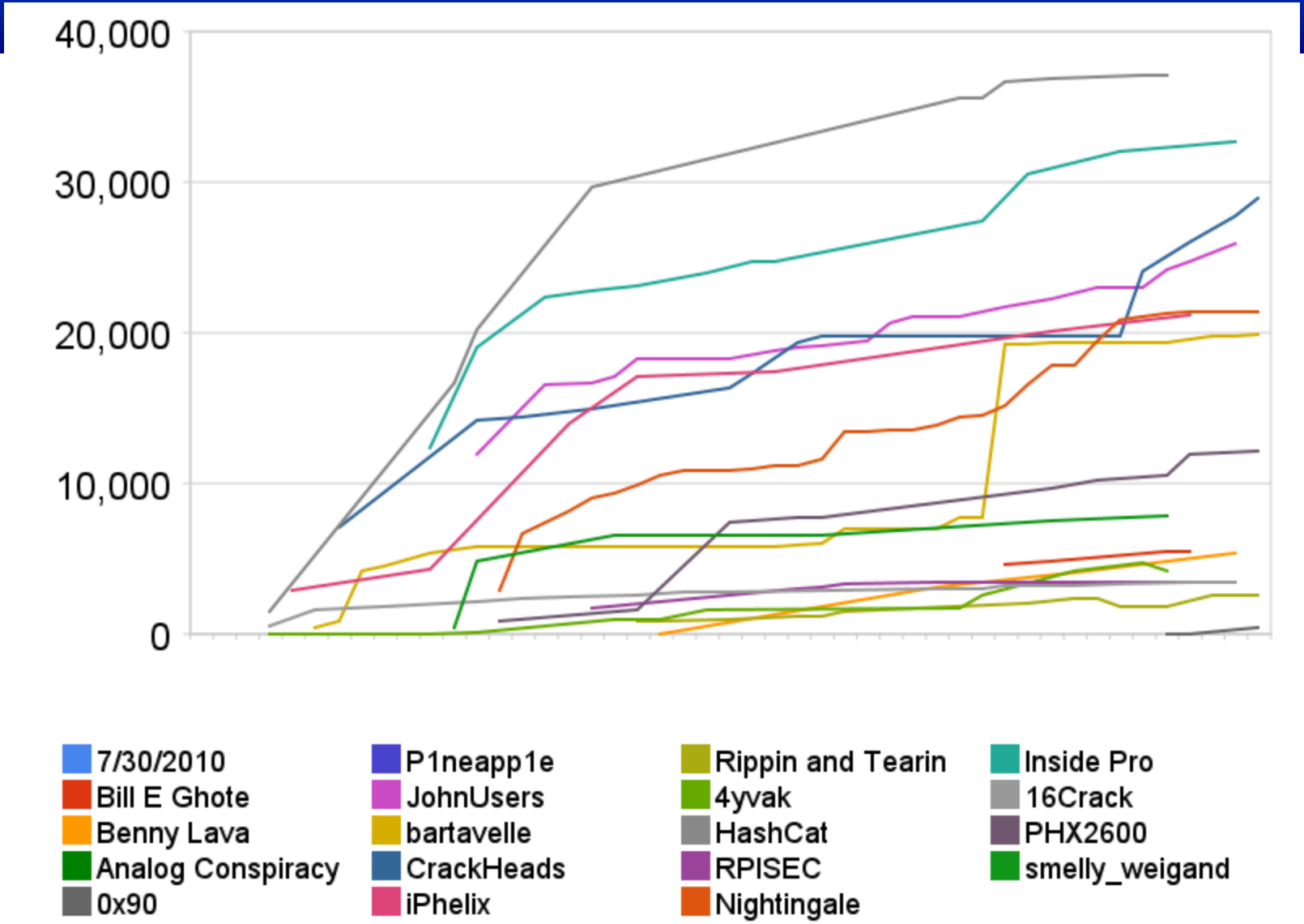
- We created ~54,000 plaintext passwords, based on every behavior we'd seen in common use within companies where we'd done pentests, ranged from very easy to very hard.
- We hashed them using the kinds of encryption types we actually see in corporations—Windows LanMan & NTMD4, UNIX DES, FreeBSD MD5, SHA and Salted SHA used by LDAP servers, etc.
- A percentage of these could be cracked using rainbow tables, “dumb” brute force, etc.
- But most couldn't. The only way to win was to be smart.

DEFCON Crack Me If You Can 2010

The goal of the contest was simple: Crack the most passwords in a 48-hour period, using any resources the teams had legitimate access to, including remote computers and members.

The catch was, in order to win they had to be willing to “show their work”: write up their methodology, and publish it to the world.

DEFCON Crack Me If You Can 2010



KoreLogic SECURITY

DEFCON Crack Me If You Can 2010

The bottom line: it worked!

- Teams did creative problem-solving, figured out the behavior patterns we had embedded in the data.
- Some new software was developed by teams on-the-fly, which was later released.

Also, afterwards we released a whole bunch of specialized dictionaries and password cracking rulesets (for John the Ripper and for the Hashcat suite) that had gone into creating the plaintexts.

You can read more about the 2010 contest, including our rulesets, and writeups from the teams at:

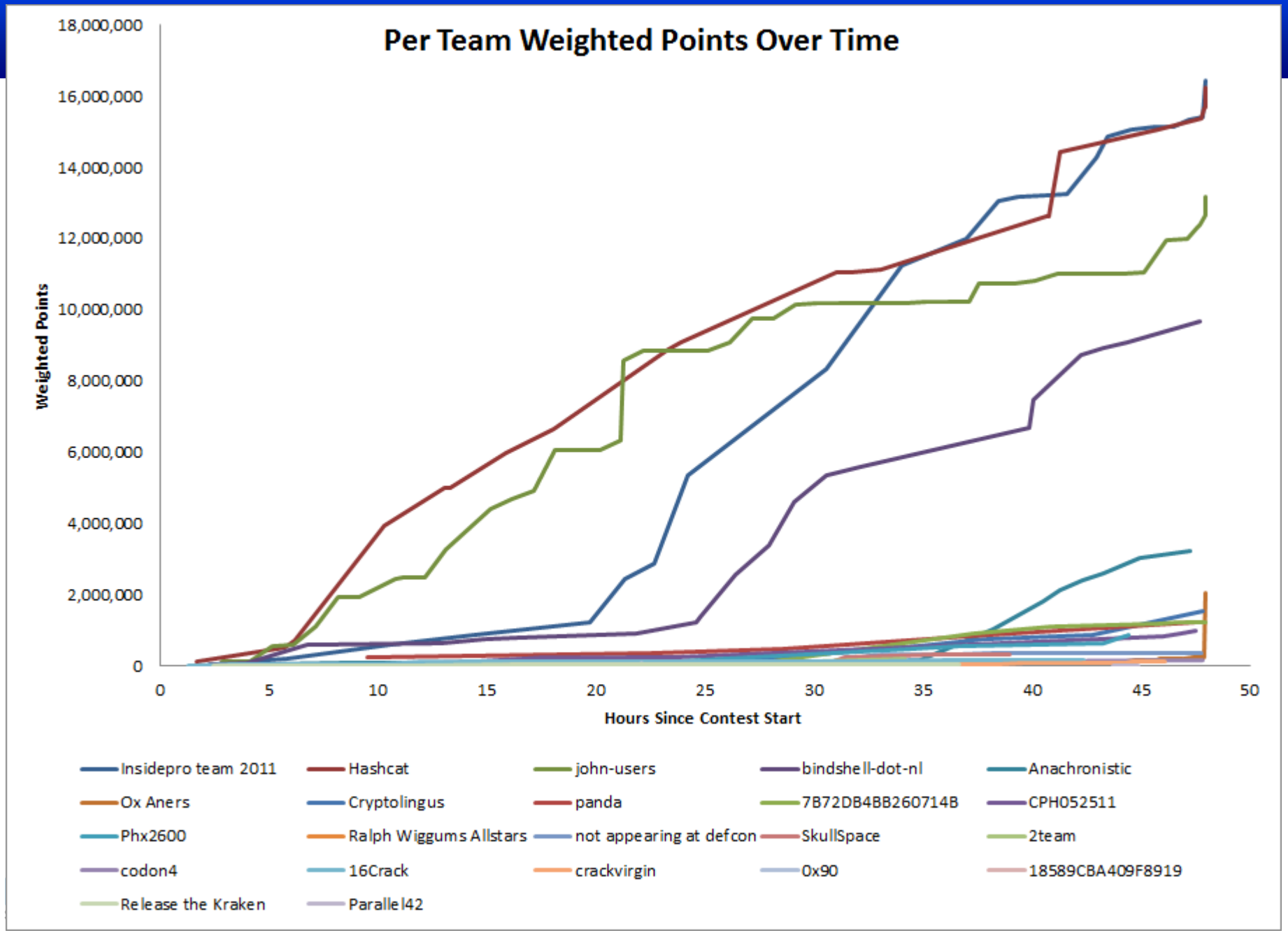
http://contest-2010.korelogic.com/

DEFCON Crack Me If You Can 2011, 2012, 2013

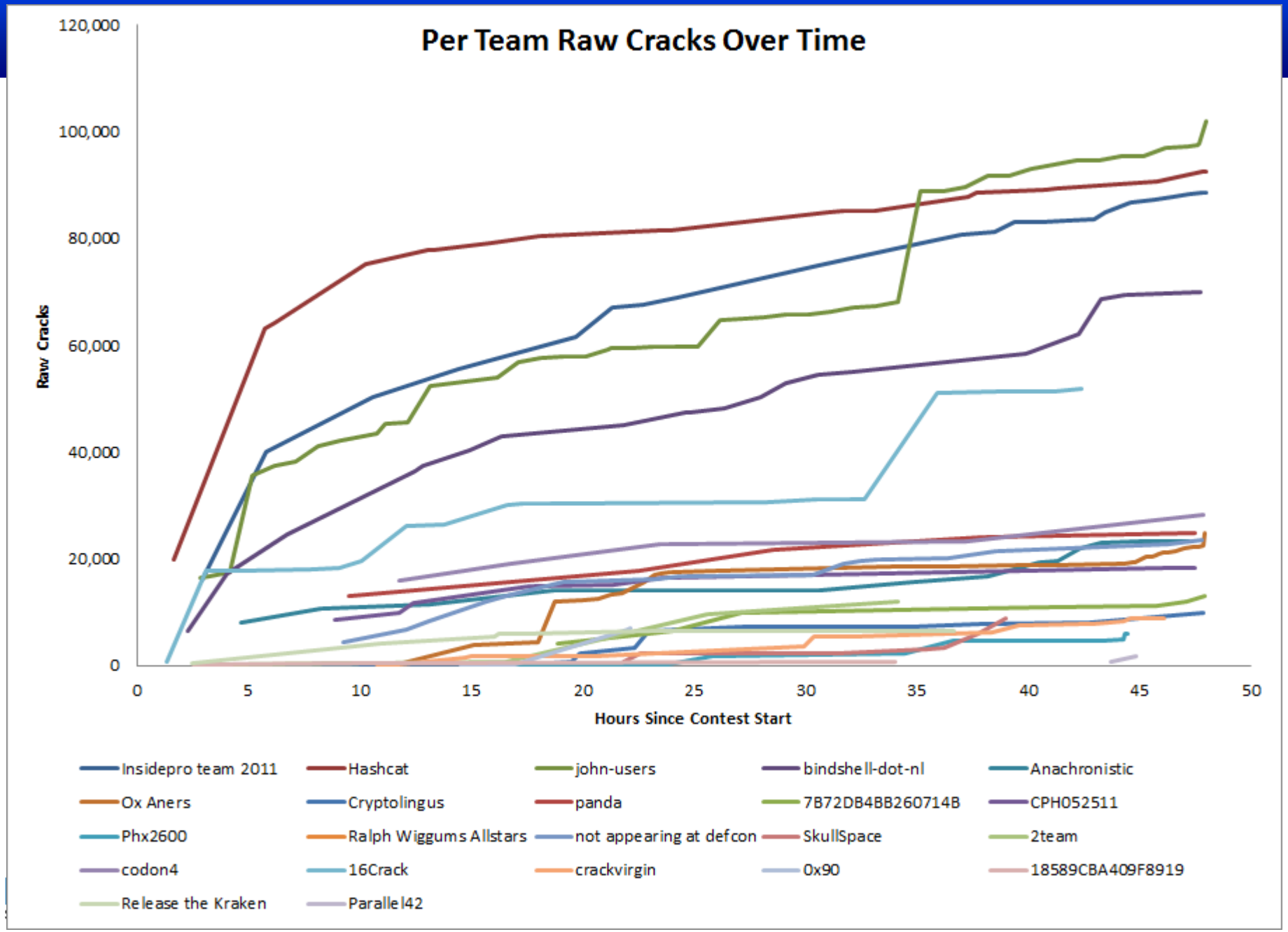
We've run the contest every year since; each time we put a slightly new spin on things:

- 2011: Introduced simple passphrases; awarded more points for harder hash types. Added hash types and encrypted container files we knew tools didn't support, to challenge them.
- 2012: More encrypted file types and longer passphrases (because many tools maxed out at 15 characters).
- 2013: Divided into “Pro” and “Street” brackets. More hash types that are not well supported. And, we introduced hash sets crafted to avoid topology reuse, to see if anyone noticed.

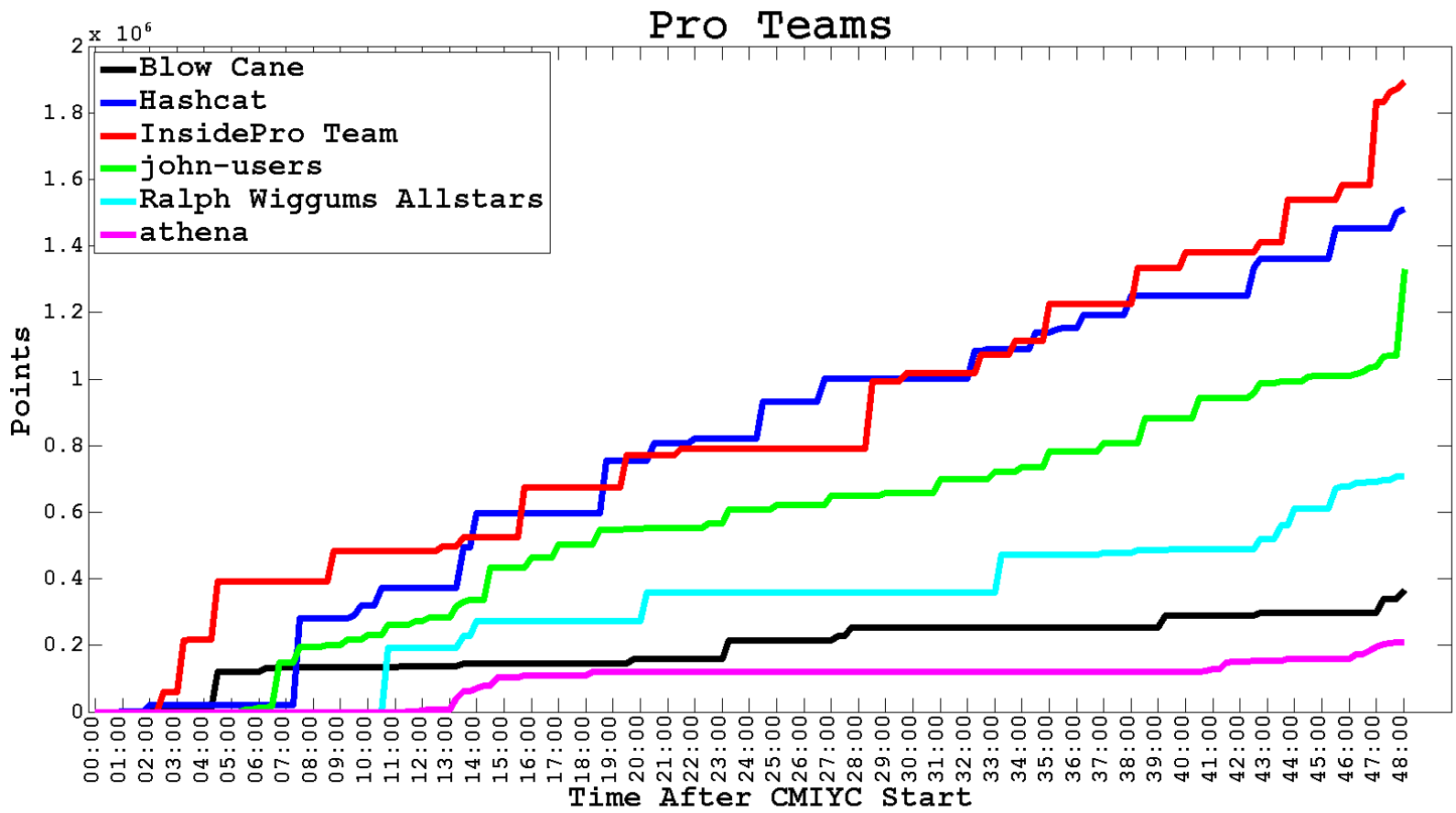
DEFCON Crack Me If You Can 2011



DEFCON Crack Me If You Can 2011

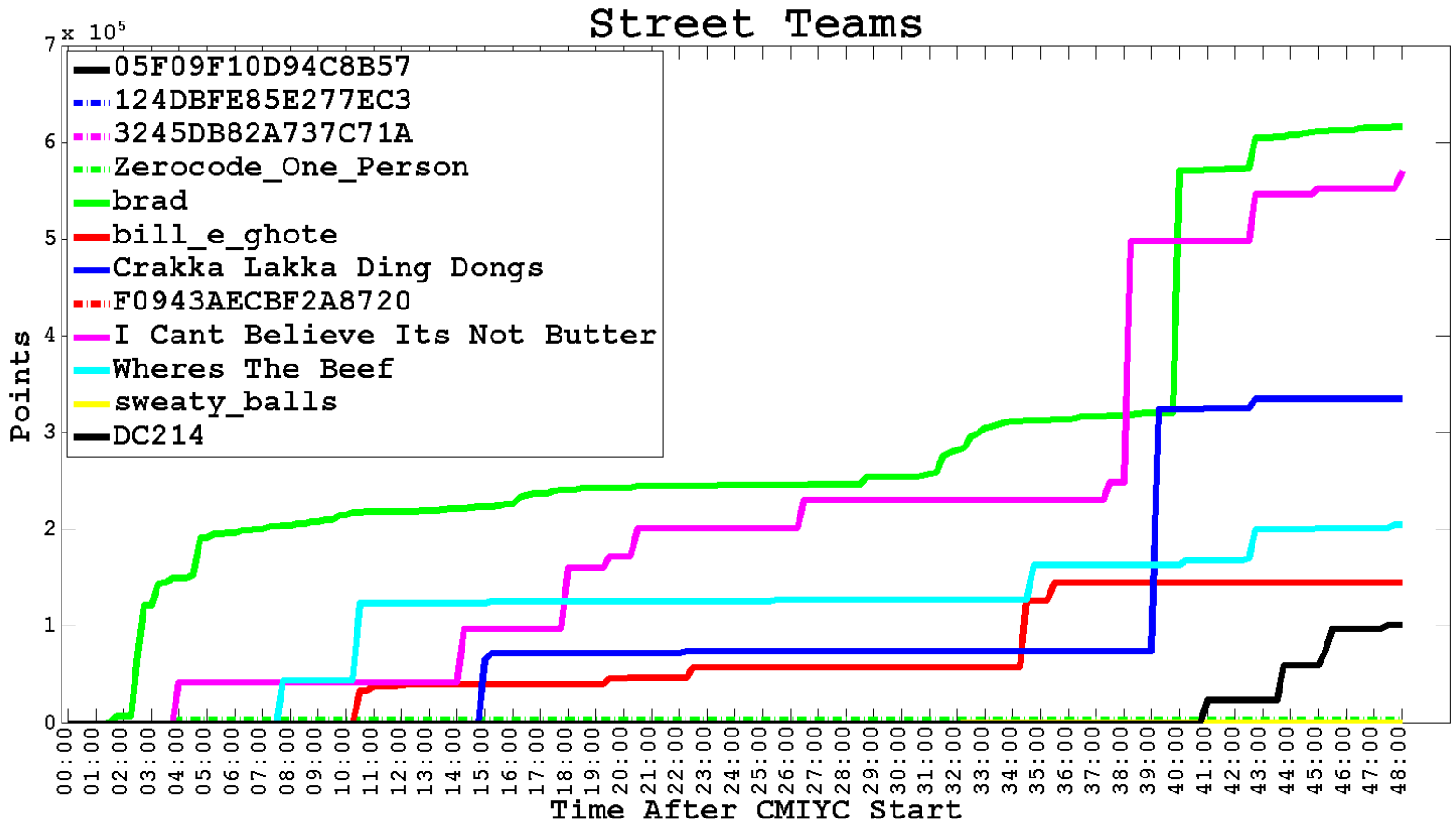


DEFCON Crack Me If You Can 2013



KoreLogic SECURITY

DEFCON Crack Me If You Can 2013



KoreLogic SECURITY

Other Reading

- https://blog.korelogic.com/
- @CrackMeIfYouCan on Twitter
- The writeups from teams that competed in the different CMIYC events:
  - http://contest-2013.korelogic.com/
  - http://contest-2012.korelogic.com/
  - http://contest-2011.korelogic.com/
  - http://contest-2010.korelogic.com/
- My coworker Rick Redman has given a number of talks about advanced password cracking techniques:
  - Passwords13: http://www.youtube.com/watch?v=5i_lm6JntPQ
  - ISSA: http://infosec-summit.issa-balt.org/html/2010_agenda.html
- Rick goes into much more detail about advanced John the Ripper techniques, the various rules we've written for it, and how to write your own.
- An interesting study about studying password selection: “On The Ecological Validity of a Password Study”: http://cups.cs.cmu.edu/soups/2013/proceedings/a13_Fahl.pdf
- PathWell, some defensive tools that KoreLogic has been developing under DARPA's CyberFastTrack program that are awesome but which I can't talk about yet :-P

Questions

Hank Leininger <hlein@korelogic.com>

KoreLogic SECURITY

Counterfeiting

Presentation slides have intentionally been omitted

Virginia Information Technologies Agency

Data Point Deep Dive

Michael Watson
Chief Information Security Officer

ISOAG
October 2, 2013

Agenda

- Packet overview
- Review data sources
  - Where we pull the data from
- Review data points
  - Identify requirements for each data point
- Review documentation
  - Identify reports that support the data points
- How does this impact my agency?

What is in the packet?

- Data points on the coversheet
  - They may not match expected values
  - Based on the entire calendar year (2013)
- Reports include actionable issues for agencies
- Supporting documentation for each data point

What is not in the packet?

- Full list of sensitive systems
  - Available upon request if needed
- Information not in the packet will be provided to the agency at a later date
  - Corrective Action Plan information
  - Quarterly Update information
  - IDS Report Submission information

Reminders

- For agencies required to use CETR
  - All system names submitted to CSRM must exist within CETR
  - If the system does not exist the agency will not get credit for the work they've done in the data points
- For agencies not required to use CETR
  - The list of systems within submitted documentation will make up the agency system list

Reminders

- The information is based on data submitted to CSRM
- This data will be used to make decisions about your agency, please make sure it is correct
- We will work with agencies as much as possible so please let us know if you identify any issues
- Specific data is now required for BIA and RA to be considered complete

ISO Certification

- Purpose
  - Set a baseline understanding for ISOs of how the Commonwealth information security program functions
- Metric
  - Minimum set of education requirements
  - Informed regarding information security issues affecting the Commonwealth

ISO Certification Status

- Requirements are listed in the cover document
- Details are included in the ISO Certification Details
  - One of the requirements could not be met until today
- Communications have been sent regarding ISO Certification Status

IT Security Audit Program

- Purpose
  - Provide a review of COV sensitive data and systems to ensure the appropriate security controls are in place and effective
  - Ensure that identified security issues are resolved and/or risk is monitored
- Metric
  - IT databases and systems are audited once every three years
  - Agencies are planning to perform sensitive system audits once every three years
  - Findings are being resolved timely or if not resolved, risks have been accepted

IT Security Audit Program Reports

- Scheduled IT Security Issues
  - List of scheduled audits that require some action
    - Overdue – Indicated by “Scheduled Audit Completion” date that has passed
    - Couldn’t map to CETR – Indicated by “Returned to Submitter” review status
    - All audits are not complete – Indicated by “All Audits Complete” set to “No”
- Sensitive Systems Missing IT Security Audits
  - Listed as a sensitive system in CETR or submitted Audit Plan
  - “Last IT Security Audit” field is older than 3 years or does not have a date

Business Impact Analysis

- Purpose
  - To identify the level of impact systems have to agency business
  - To identify the level of impact systems have to the Commonwealth as a whole
- Metric
  - All business processes must be rated for impacted
    - Life, safety, regulatory, etc.
  - All business processes must have an identified Recovery Time Objective (RTO)
  - All business processes must be labeled as mission essential or not mission essential
  - All applications must be associated with a business process

Business Impact Analysis Reports

- Actionable Business Processes
  - Business process does not have a rating
  - A recovery time objective is not set or is 0
  - Mission essential status is not identified
- Applications Associated with a Business Function
  - Application does not have an associated rated business process

Risk Assessment

- Purpose
  - Assess COV sensitive data and systems for risks to agency business
  - Ensure that identified risks are resolved and/or monitored
- Metric
  - Systems have been assessed within the last 3 years
  - Findings are being resolved timely or if not resolved, risks have been accepted

Risk Assessment Reports

- Sensitive Systems Missing a Risk Assessments
  - Sensitive systems that have a “Last Scheduled Agency IT Risk Assessment” over 3 years ago
- Agency Application Risk Assessment Status
  - Sensitive systems along with the dates of their “Last Scheduled Agency IT Risk Assessment” and their “Next Scheduled Agency IT Risk Assessment”
- Critical Systems Missing an IT Risk Assessment
  - Systems with a “Criticality” of high that do not have a risk assessment within the last 3 years

Findings

- Purpose
  - Track identified security issues from identification to completion
- Metric
  - Findings are resolved in a reasonable time period
  - Findings have remediation plans
  - Findings are making progress towards remediation

Findings Reports

- Overdue Findings
  - Findings identified as being past their "Estimated due date"

What do I do if I'm Red?

- Respond with a risk recommendation with a plan to be green
- Updates on risk remediation progress will be required
- Ensure agency leadership is informed
- Talk to your analyst

Future Use

- Risk recommendations
  - Risk management standard
  - Agencies on track to be red for 2013
- IT strategic planning
- Operational control implementation

Future Plans

- Rollout of tool should be finished by the end of the year
- Agencies will have access to electronic copies of these reports and more
- Data point information will be provided electronically going forward
- ISOs will have access by default

Questions?

Virginia Information Technologies Agency

End of Life Software: Considerations and Controls

Bob Baskette

Senior Manager, Security Operations and Architect

End of the Line

- Every COV Agency has software within its environment that is considered End-of-Life or End-of-Support by the software vendor.

- Some EOL software is required to support legacy applications while other software is simply a legacy item.

EOL Issues

- Vulnerabilities remain long after the vendor stops providing patches.
- Source code and installation media fade away.
- Developers often retire before the systems do.

EOL Issues

- Old software and new hardware simply do not understand each other.

- License Keys are difficult to track and therefore upgrades are difficult to achieve.

Microsoft Server OS

OS	EMS	EOL
Server 2003	7/13/2010	7/14/2015
Server 2008	1/13/2015	1/14/2020
Server 2012	1/9/2018	1/10/2023

EMS = End of Mainline Support

EOL = End of Life/Extended Support

Microsoft Desktop OS

OS	EMS	EOL
Windows XP	4/14/2009	4/8/2014
Windows Vista	4/10/2012	4/11/2017
Windows 7	1/13/2015	1/14/2020
Windows 8	1/9/2018	1/10/2023

Microsoft SQL Server Software

	EMS	EOL
Server 2000	4/8/2008	4/9/2013
Server 2005	4/12/201	4/12/2016
Server 2008	7/8/2014	7/9/2019
Server 2012	7/11/2017	7/12/2022

Microsoft SQL Server Software

	EMS	EOL
Server 6.0	3/31/1999	Not Applicable
Server 6.5	1/1/2002	Not Applicable
Server 7.0	12/31/2005	1/11/2011

Red Hat Support Levels

Production 1 PhaseIV:

- Includes qualified Critical and Important Security errata advisories (RHSAs) and Urgent and Selected High Priority Bug Fix errata advisories (RHBAs)

- Other errata advisories may be delivered as appropriate.

Red Hat Support Levels

Production 1 PhaseIV:

- Includes new or improved hardware enablement and select enhanced software functionality

- Includes Minor software releases as well as qualified errata advisories (RHSAs, RHBAs, and RHEAs).

Red Hat Support Levels

Production 2 PhaseV:

- Includes qualified Critical and Important Security errata advisories (RHSAs) and Urgent Priority Bug Fix errata advisories (RHBAs)

- Hardware enablement that does not require substantial software changes may be provided at the discretion of Red Hat

Red Hat Support Levels

Production 2 PhaseV:

- New software functionality is not available during this phase.

- Minor releases will also include all available and qualified errata.

Red Hat Support Levels

Production 2 PhaseV:

- The focus for minor releases during this phase lies on resolving urgent- or high-priority bugs.

- Updated installation images will be provided only if required because of installer changes.

Red Hat Support Levels

Production 3 PhaseVI:

- Includes Critical Impact Security Advisories (RHSAs) and selected Urgent Priority Bug Fix Advisories (RHBAs)

- Other errata advisories may be delivered as appropriate.

Red Hat Support Levels

Production 3 PhaseVI:

- New functionality and new hardware enablement are not planned for availability.

- Minor releases with updated installation images may be made available.

Red Hat Support Levels

Extended Life Phase:

- Includes access to previously released content on the Red Hat Customer Portal

- Also includes critical impact security fixes and selected urgent-priority bug fixes.

Red Hat Enterprise Linux 3

General Availability	10/23/2003
End of Production 1	7/20/2006
End of Production 2	6/30/2007
End of Production 3	10/31/2010
End of Life	1/30/2014

Red Hat Enterprise Linux 4

General Availability	2/14/2005
End of Production 1	3/31/2009
End of Production 2	2/16/2011
End of Production 3	2/29/2012
End of Life	2/28/2015

Red Hat Enterprise Linux 5

General Availability	3/15/2007
End of Production 1	1/8/2013
End of Production 2	1/31/2014
End of Production 3	3/31/2017
End of Life	Q1 of 2020

Red Hat Enterprise Linux 6

General Availability	11/10/2010
End of Production 1	Q2 of 2016
End of Production 2	Q2 of 2017
End of Production 3	11/30/2020
End of Life	Q4 of 2023

Adobe ColdFusion Software

	EMS	EOL
ColdFusion 10	5/16/2012	5/16/2019
ColdFusion 9	12/31/2014	12/31/2016
ColdFusion 8	7/31/2012	7/31/2014
ColdFusion 7	2/7/2010	2/7/2012

Adobe Acrobat Software

	EMS	EOL
Acrobat XI Pro 11	10/15/2017	N/A
Acrobat XI Std 11	10/15/2017	N/A
Acrobat X Pro 10	11/15/2015	N/A

Adobe Acrobat Software

	EMS	EOL
Acrobat X Std 10	11/15/2015	N/A
Acrobat X Suite 10	11/23/2015	N/A
Acrobat Pro 9.x	6/26/2013	N/A
Acrobat Std 9.x	6/26/2013	N/A

Adobe Acrobat Software

	EMS	EOL
Acrobat 3D 8.x	11/3/2011	N/A
Acrobat Pro 8.x	11/3/2011	N/A
Acrobat Std 8.x	11/3/2011	N/A

Adobe Acrobat Software

	EMS	EOL
Acrobat Elements 7	4/6/2010	N/A
Acrobat Pro 7	12/28/2009	N/A
Acrobat Std 7	12/28/2009	N/A

Adobe Reader Software

	EMS	EOL
Reader X 10	11/18/2015	N/A
Reader XI 11	10/15/2017	N/A
Reader 9	6/26/2013	N/A

Adobe Reader Software

	EMS	EOL
Reader 8	11/3/2011	N/A
Reader 7	12/28/2009	N/A

Oracle Database Software

	EMS	EOL
Oracle 11.1.0.X	8/2012	8/2015
Oracle 10.2.0.X	7/2010	7/2013
Oracle 10.1.0.X	1/2009	1/2012
Oracle 9.2.0.X	7/2007	7/2010

Oracle Solaris Unix

	EMS	EOL
Solaris 8	3/2009	3/2012
Solaris 9	10/2011	10/2014
Solaris 10	1/2018	1/2021
Solaris 11	11/2021	11/2024

Oracle Solaris Linux

- Solaris 9
  - The last update for Solaris 9 was 9/05
  - Extended Support for Solaris 9 ends in October, 2014. After which it enters in Sustaining Support phase.

- Solaris 8
  - The last update for Solaris 8 was 2/04
  - Solaris 8 is in Sustaining Support phase of its life cycle.

Oracle Sustaining Support

- May be offered for an indefinite period.
- Provides continued access to technical experts, online tools, and knowledgebase resources.
- Can provide updates, patches, fixes, security patches and security alerts created during the Oracle Premier Support period.

Oracle Sustaining Support

- Does not provide new program updates, patches, fixes, security patches, security alerts, general maintenance releases, selected functionality releases, documentation updates, or upgrade tools.

Oracle Unbreakable Linux

	EMS	EOL
Linux 3	10/2011	N/A
Linux 4	2/2013	N/A
Linux 5	3/2017	N/A
Linux 6	3/2021	N/A

EOL Considerations

- Section SI-2-COV of ITRM COV SEC 501-07 requires the organization to:
  - a. Applies all software publisher security updates to the associated software products.
  - c. Prohibits the use of software products that the software publisher has designated as End-of-Life/End-of-Support (i.e. software publisher no longer provides security patches for the software product).

EOL Controls

- EOL software requires compensating controls to protect the environment.
  - Deploy Integrity Control software to prevent system-level changes
  - Remove all unneeded/unnecessary software and services
  - Configure firewall rules to block all unneeded/unnecessary ports and protocols
  - Remove all unneeded accounts
  - Set all required accounts to the minimal privilege level

EOL Paperwork

- To continue the use of EOL software an Agency will need to submit the following paperwork:
  - Security Exception Request for Section SI-2-COV of ITRM COV SEC 501-07
  - Documentation of installed system integrity controls
  - Remediation plan to decommission the EOL software

Questions???

For more information, please contact:
CommonwealthSecurity@vita.virginia.gov

Thank You!

Virginia Information Technologies Agency

2013 Penetration Test

Bob Baskette

Senior Manager, Security Operations and Architect

2013 Penetration Test

This Presentation Has Intentionally Been Omitted

Upcoming Events

Information Security System Association

ISSA

DATE: Wednesday, October 9, 2013

LOCATION: Maggiano's Little Italy
11800 West Broad Street, #2204, Richmond, VA 23233
TIME: 11:30 - 1:00pm. Presentation starts at 11:45.
Lunch served at 12.
COST: ISSA Members: $20 & Non-Members: $25

SPEAKER: Randy Grubb

TOPIC: *Tug A War: Privacy & Data in the Digital Age*
More info located here: http://centva.issa.org/central-va-issa-feb-2013-meeting/

Virginia Information Technologies Agency

Cyber Security Awareness Month

Everyone is welcome to attend!!

Date: October 8, 2013
Speaker: Ed Miller, VITA
Topic: Social Media Risk
Time: 12pm – 1pm
Location: CESC Room 1222

Date: October 16, 2013 ***Cyber Security Awareness Day***
Speaker: Peter Miller, Chief Privacy Officer, Federal Trade Commission
Topic: Privacy & Identity Theft
Time: 12pm – 1pm
Location: CESC Room 1223

Date: October 30, 2013
Speaker: SA John Houlberg, VSP
Topic: Internet Safety for Children
Time: 12pm – 1pm
Location: CESC Room 1223

Virginia Information Technologies Agency

DOA Training Offering

Auditing the Internal Network

Instructor: David Cole (SysAudits)

Date: October 29 & 30, 2013

Time: 8:15-4:45

Location: James Monroe Building

Conf. Rm. B, 1st FL

Cost: $ 320.00

Register: https://hrtraining.doa.virginia.gov/

Virginia Information Technologies Agency

Future ISOAG

Nov 6	**1:00 – 4:00 pm @ CESC**
Keynote Speaker:	**David Ihrie, Center for Innovative Technology on "CIT Cyber Security Accelerator"**
Dec 4	**1:00 – 4:00 pm @ CESC**
Keynote Speaker:	**John McLain, Grant Thorton, LLP on "Cloud Security"**

ISOAG meets the 1st Wednesday of each month in 2013

Virginia Information Technologies Agency

IS Orientation

When: Thursday, Dec 5, 2013

Time: 10:00 am to Noon

Where: CESC , Room 1221

Register here:

http://vita2.virginia.gov/registration/Session.cfm?MeetingID=10

Next IS Orientation will be held on Mar 9, 2014

Virginia Information Technologies Agency

Save The Date

IT Security Conference

"Information Security Enabling the Business"

Date: April 2,3 & 4, 2014

The event will include numerous topics and a SANS class on Mobile Device Security.

More details will be provided soon!

Submit Events

- If your group or organization is promoting a security related event and would like to have it communicated to the Information Security Officer community:

Please submit all upcoming events to: **CommonwealthSecurity@VITA.Virginia.Gov**

ISOAG-Partnership Update

IT Infrastructure Partnership Team
Bob Baskette

2 October, 2013

IT INFRASTRUCTURE PARTNERSHIP

VITA

NORTHROP GRUMMAN

ADJOURN

THANK YOU FOR ATTENDING