



The Nature of Cyber Security

Eugene H. Spafford

PURDUE
UNIVERSITY



Presented as Keynote #2 at

WORLDCOMP'11 – The 2011 World Congress in Computer Science, Computer Engineering, and Applied Computing

The Monte Carlo Resort and Casino, Las Vegas, NV, 18 July 2011

Thanks to Dr. Fariborz Farahmand for assistance with background research used in this presentation.

Contact information for Professor Spafford may be found at <http://spaf.cerias.purdue.edu>



The Environment

The Environment



The screenshot shows the Infosec Island website header and a news article. The header includes the Infosec Island logo with palm trees, the text "SCADA Security and Compliance Platform", and a navigation menu with links: Front Page | Blog Posts | Downloads | Videos | From the Web | Forums | Free Tools | Breaches | Vuln. The main article title is "RSA SecurID Breach Spreads to L3 and Northrop", dated Thursday, June 02, 2011. The article begins with "Contributed By:" followed by a partially visible sentence: "While few details have ever been released that could give analysts an".

The Environment



Monday, October 18, 2010 As of 12:00 AM

THE WALL STREET JOURNAL. | WHAT THEY KNOW

[U.S. Edition Home](#) | [Today's Paper](#) | [Video](#) | [Blogs](#) | [Journal Community](#)

[World](#) | [U.S.](#) | [New York](#) | [Business](#) | [Markets](#) | [Tech](#) | [Personal Finance](#) | [Life & Culture](#)

[Digits](#) | [Personal Technology](#) | [What They Know](#) | [All T](#)

[Front Page](#) | [Bl](#)

RSA Se

Thursday, J

Contributed

WHAT THEY KNOW | OCTOBER 18, 2010

Facebook in Privacy Breach

Top-Ranked Applications Transmit Personal IDs, a Journal Investigation Finds

Article | Video | Comments

The Environment



HOME PAGE | TODAY'S PAPER | VIDEO | MOST POPULAR | TIMES TOPICS

The New York Times **Business Day**

WORLD | U.S. | N.Y. / REGION | BUSINESS | TECHNOLOGY | SCIENCE | HEALTH | SPORTS | OPINION | Personal Finance | Life & Culture

Search | Global | DealBook | Markets | Economy | Personal Technology | **What They Know** | All T

RSA Faces Angry Users After Breach

By NELSON D. SCHWARTZ and CHRISTOPHER DREW
Published: June 7, 2011

The nation's biggest banks and large technology companies like SAP
rushed Tuesday to accept RSA Security's offer to relogin their

RECOMMEND

Facebook in Privacy Breach

Top-Ranked Applications Transmit Personal IDs, a Journal Investigation Finds

Article | Video | Comments



The Environment

The screenshot displays two overlapping web pages. The background page is The New York Times, with a navigation bar including 'HOME PAGE', 'TODAY'S PAPER', 'VIDEO', 'MOST POPULAR', and 'TIMES TOPICS'. The main headline reads 'RSA Faces Angry Users Af...' by Nelson D. Schwartz and Christopher Drew, published on June 7, 2011. The foreground page is Ars Technica, featuring a dark red header with the 'ars' logo and 'ars technica' text. A secondary navigation bar includes categories like 'ALL', 'APPLE', 'ASK ARS', 'BUSINESS', 'GADGETS', 'GAMING', 'MICROSOFT', and 'OPEN SOURCE'. Below this, there are links for 'NEWS', 'GUIDES', and 'REVIEWS', along with a 'Upgrade to a Premi...' button. The main article on Ars Technica is titled 'Sony: Anonymous provided cover for PSN attack' by Ben Kuchera, published 2 months ago. A prominent orange banner above the article reads 'Opposable Thumbs' with a play button icon and the text 'What you need to know to play'.



The Environment

The screenshot displays the homepage of The Register, a technology news outlet. The main navigation bar includes categories such as Hardware, Software, Music & Media, Networks, Security, Cloud, Public Sector, Business, and Science. A secondary navigation bar lists specific topics like Crime, Malware, Enterprise Security, Spam, and ID. The featured article is titled "North Korea blamed for bank hack" with the subtitle "Hackers not so lonely" by John Oates, published on May 3rd, 2011. Another article, "Sony: Anonymous provided cover for PSN attack" by Ben Kuchera, is also visible. The page includes social media sharing options (Print, Tweet, Like) and an Alert button. On the right side, there are promotional banners for "SOFT OPEN SOURCE" and "Upgrade to a Premium" subscription.

The Environment



HOME PAGE | TODAY'S

The Register

HELP NET SECURITY

HOME | NEWS | ARTICLES | SOFTWARE | VIDEOS | RISKS | EVENTS | BOOKSTORE | ABOUT






Infected flash drive blamed for US military breach

Posted on 26.08.2010

BOOKMARK

LATEST NEWS » Sunday, 16:23 EDT

- Vodafone femtocell hack allows call interception on unpatched devices
- New Hotmail security features against account hijacking
- Verizon takes on issue of stolen credentials
- Secure mobile device access on single authentication platform
- 90 people arrested for organized

 The most significant computer systems' breach in U.S. military history dates back to 2008, when malicious code contained in a flash drive infected a laptop of a military official posted in the Middle East, and spread further to the network of the U.S. Central Command. The code in question was put on the drive by operatives of a foreign intelligence agency, most likely Russian.

This information would have likely remain hidden to the greater public, were it not for Deputy Defense Secretary William J. Lynn III

SOFT OPEN SOURCE

Upgrade to a Premi

eed to know to play

attack

The Environment

HOME PAGE | TODAY'S

Enterprise Mobility - eWeek

SEARCH: microsoft patch tuesday

eWEEK.COM SUBSCRIBE TO eWEEK | RSS Feeds | Print | Newsletters

HOME | NEWS | REVIEWS | STORAGE | SECURITY | DESKTOPS/NOTEBOOKS | MOBILITY | CLOUD COMPUTING | BIZ ADVISOR | BLOGS | WHITE PAPERS | WEBCASTS

Windows Interop • Apple iPhone & iTouch • Open Source • Networking • Midmarket • Messaging & Collaboration • VoIP & Telephony • Web 2.0 • Videos • All eWeek Topics

Home > Enterprise Mobility News & Reviews > Microsoft Fixes 22 Bugs in July Patch Tuesday

Mobile News

Microsoft Fixes 22 Bugs in July Patch Tuesday

By: Fahmida Y. Rashid | 2011-07-12 | Article Rating: ★★☆☆☆ / 1

There are 0 user comments on this Enterprise Mobility story.

network of the U.S. Central Command. The code in question was put on the drive by operatives of a foreign intelligence agency, most likely Russian.

This information would have likely remain hidden to the greater public, were it not for Deputy Defense Secretary William J. Lynn III

Verizon takes on issue of stolen credentials

Secure mobile device access on single authentication platform

90 people arrested for organized

Delivering Business to Your Customers

Watch Now >

attack



The Environment

The screenshot shows the ABC News Technology website. At the top, there are navigation links for 'HOME PAGE' and 'TODAY'S'. The main header includes the 'abc NEWS / Technology' logo, a 'HOT TOPICS' section with links to 'Casey Anthony', 'Elin Nordegren', and 'Harry Potter', and a search bar. Below the header is a navigation menu with categories like 'Home', 'Video', 'News', 'Politics', 'Investigative', 'Health', 'Entertainment', 'Money', 'Tech', 'World News', and 'Nightline'. A secondary navigation bar includes 'BLOGS', 'WHITE PAPERS', and 'WEBCASTS'. The main content area features a headline: 'Top Hacker Suspect Arrested After Attacks on Sony, Sega, Citibank, CIA'. To the right, there is a 'SEARCH' bar with the text 'microsoft patch tuesday' and a 'ZIFF BARRIS enterprise' logo. Below the headline, there is a list of bullet points: 'Verizon takes on issue of stolen credentials', 'Secure mobile device access on single authentication platform', and '90 people arrested for organized'. The article text is partially obscured by a black redaction box. On the right side, there is a 'day's Featured Video' section with a video thumbnail titled 'Delivering Business to Your Customers' and a 'Watch Now' link. At the bottom right, the word 'attack' is visible.

The Environment



The screenshot shows the eWEEK.com website interface. At the top, there are navigation links for 'HOME PAGE' and 'TODAY'S'. The main header features the 'abc NEWS / Technology' logo and a 'HOT TOPICS' section listing Casey Anthony, Elin Nordegren, and Harry Potter. A search bar contains the text 'microsoft patch tuesday'. Below this, there is a sub-header for 'IT Security & Network Security News & Reviews' with another search bar containing 'oracle patch'. The eWEEK.COM logo is prominent, along with navigation tabs for various categories like NEWS, REVIEWS, STORAGE, SECURITY, etc. The main article is titled 'Oracle Plans 78 Bug Fixes in Critical Patch Update' by Fahmida Y. Rashid, dated 2011-07-15. It includes social media sharing buttons for LinkedIn, Facebook, Twitter, and ShareThis. A video player on the right shows a featured video titled 'Delivering Business to Your Customers' with a duration of 03:23. An editorial calendar sidebar is also visible on the left.

The Environment

The screenshot shows the ABC News Technology section. The main article is titled "Security breach: Hackers steal 90,000 US military email IDs". The article is dated July 13, 2011, at 12:26am IST. The byline is Fahmida Y. Rashid, dated 2011-07-15. The article rating is 1 out of 5 stars. The article text begins with "WASHINGTON: Hackers claim to have stolen over 90,000 email".

Navigation links include: HOME PAGE, TODAY'S, SEARCH (microsoft patch tuesday), HOT TOPICS (Casey Anthony, Elin Nordegren, Harry Potter), SEARCH, THE TIMES OF INDIA | US, Home, City, India, World, Business, Tech, Sports, Entertainment, Life & Style, Women, Hot on the Web, NRI News, Travel deals, US, Pakistan, South Asia, UK, Europe, China, Middle East, Rest of World, Mad, Mad World, You are here: Home > Collections, RELATED ARTICLES, Internet hackers claim attack on FBI partner in Connecticut, Update, LinkedIn 0, Share 0, Tweet 2, +1 0, ShareThis 3, For a list of what eWEEK is covering this year, visit our editorial calendar., WEBCASTS, All Videos, Delivering Business to Your Customers Watch Now>.

The Environment



The screenshot displays a collage of news website interfaces. At the top left, the ABC NEWS / Technology logo is visible. To its right, a 'HOT TOPICS' section lists Casey Anthony, Elin Nordegren, and Harry Potter. Further right is a search bar with the text 'microsoft patch tuesday'. Below these, the news.com.au logo is prominent, featuring the tagline 'FROM ALL ANGLES'. A navigation menu includes categories like News, Business, Money, Entertainment, Travel, Technology, Blogs, and Video. A sub-menu highlights 'National', 'World', 'Weird', 'Weather', 'Multimedia', and 'Pictures'. The main article headline reads 'Investigation into South Australia's Medvet lab after serious privacy breach', attributed to Sarah Martin, dated July 18, 2011, at 12:00am. Social media sharing icons for Facebook, Twitter, and LinkedIn are present. On the left side of the collage, a snippet from 'THE TIME' is visible, along with a 'RELATED ARTICLE' section titled 'Internet hackers claim...' and a small graphic for an 'eWEEK' editorial calendar.

The Environment

HOME PAGE | TODAY'S



THE TIME

Home City India World

US Pakistan South Asia

You are here: Home > Colle

RELATED ARTICLE

[Internet hackers claim a](#)
[Connecticut](#)

For a list of what eWEEK is covering this year, visit our [editorial calendar](#).

Sign Out Print Subscription Conversations Today's Paper

POLITICS OPINIONS LOCAL SPORTS **National** World Business Investigations

tuesday

rise

body+so

Search

The Washington Post

NATIONAL

Corrections Energy & Environment Health & Science Higher Education National Security On Fal

In the News Jennifer Lopez World Cup 'Carmageddon' 'Harry Potter' Casey Anthony

Checkpoint Washington

Reporting on diplomacy, intelligence and military affairs



On Twitter | E-Mail Checkpoint | More national security news | RSS Feed

ABOUT THIS BLOG

Checkpoint Washington is produced by the national security staff of The Washington Post

Posted at 04:01 PM ET, 07/11/2011

Anonymous claims it obtained military data in breach of Booz Allen systems

By [Jason Ukman](#)

The Environment

And hundreds of other incidents this year alone.

These are becoming so common that they aren't even reported as regular news.



The Magnitude



The Magnitude

- Over 8,000 publicly disclosed security-relevant flaws in software in 2010; similar pace in 2011

The Magnitude

- Over 8,000 publicly disclosed security-relevant flaws in software in 2010; similar pace in 2011
- Reported losses exceed \$500 million per year in the U.S. alone

The Magnitude

- Over 8,000 publicly disclosed security-relevant flaws in software in 2010; similar pace in 2011
- Reported losses exceed \$500 million per year in the U.S. alone
- Unreported and cyber espionage losses are at least the same amount

The Magnitude

- Over 8,000 publicly disclosed security-relevant flaws in software in 2010; similar pace in 2011
- Reported losses exceed \$500 million per year in the U.S. alone
- Unreported and cyber espionage losses are at least the same amount
- Despite aggressive actions, SPAM still outweighs normal email by a ratio of 3 to 1



- For 1st quarter 2011 malware

- For 1st quarter 2011 malware
 - Cellphone malware exceed 1000 different types

- For 1st quarter 2011 malware
 - Cellphone malware exceed 1000 different types
 - 6 million new samples for regular computers

- For 1st quarter 2011 malware
 - Cellphone malware exceed 1000 different types
 - 6 million new samples for regular computers
 - Total known exceed 60 million

- For 1st quarter 2011 malware
 - Cellphone malware exceed 1000 different types
 - 6 million new samples for regular computers
 - Total known exceed 60 million
 - Almost 1 million new password-theft Trojans

- For 1st quarter 2011 malware
 - Cellphone malware exceed 1000 different types
 - 6 million new samples for regular computers
 - Total known exceed 60 million
 - Almost 1 million new password-theft Trojans
 - Over 1.2 million unique fake antivirus programs





- So far in 2011



- So far in 2011
 - Over 300 data breach incidents disclosed with over 23 million records disclosed.

- So far in 2011
 - Over 300 data breach incidents disclosed with over 23 million records disclosed.
 - New botnet infections fell to “only” 3 million per month.

- So far in 2011
 - Over 300 data breach incidents disclosed with over 23 million records disclosed.
 - New botnet infections fell to “only” 3 million per month.
 - 1.2% of searches & 49% of trending terms led to malicious WWW sites.

- So far in 2011
 - Over 300 data breach incidents disclosed with over 23 million records disclosed.
 - New botnet infections fell to “only” 3 million per month.
 - 1.2% of searches & 49% of trending terms led to malicious WWW sites.
 - 2500 new phishing sites per day.



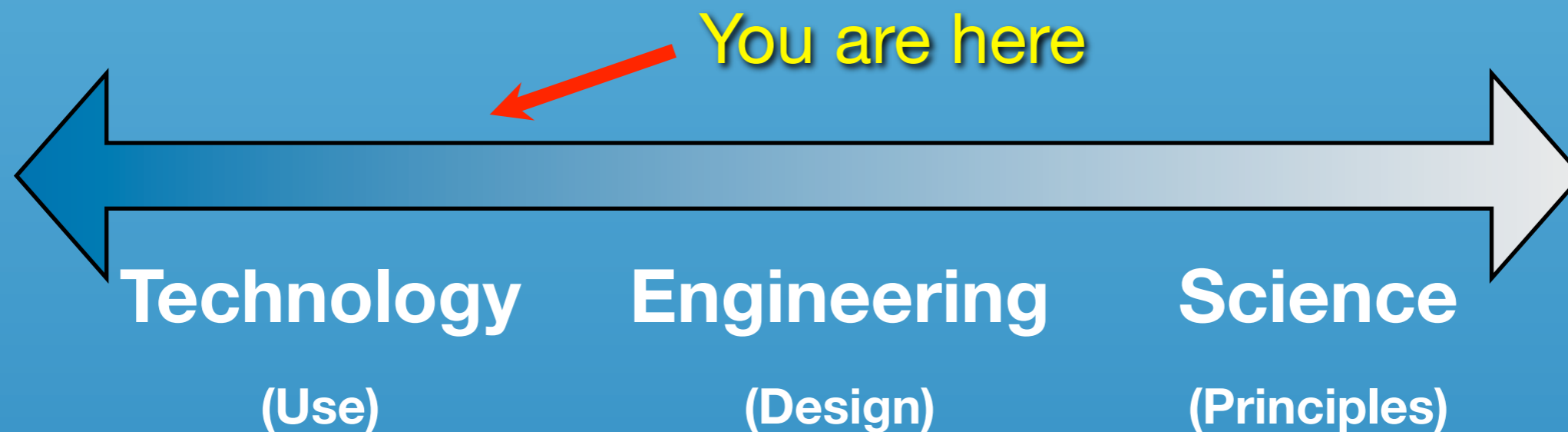
Clearly, there is a problem

Clearly, there is a problem

- But it isn't new!
- Some of us have been sounding the alarm for over 20 years.
- Spending on cyber security in the U.S. alone exceeds \$8 billion a year but we are still falling behind.

One contention

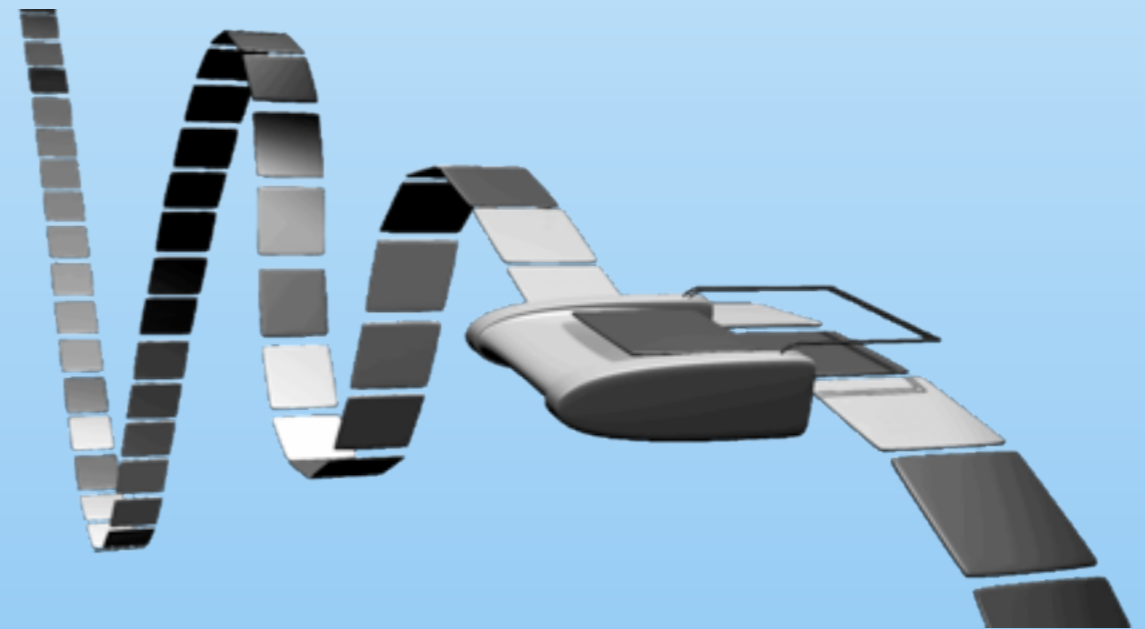
Our approach has been based on *ad hoc* practice rather than formal science



Hey, we do science! ...don't we?



- Science is the formulation of hypotheses, experimentation, and analysis
- Experiments must be repeatable and subject to refutation





How often do you see
accounts of experiments
redone by others?

When did you last see
negative results published?

How often do you see
accounts of experiments
redone by others?

How many security papers have you seen with a formal null hypothesis, full listing of procedures and equipment, and statistical analysis of data?

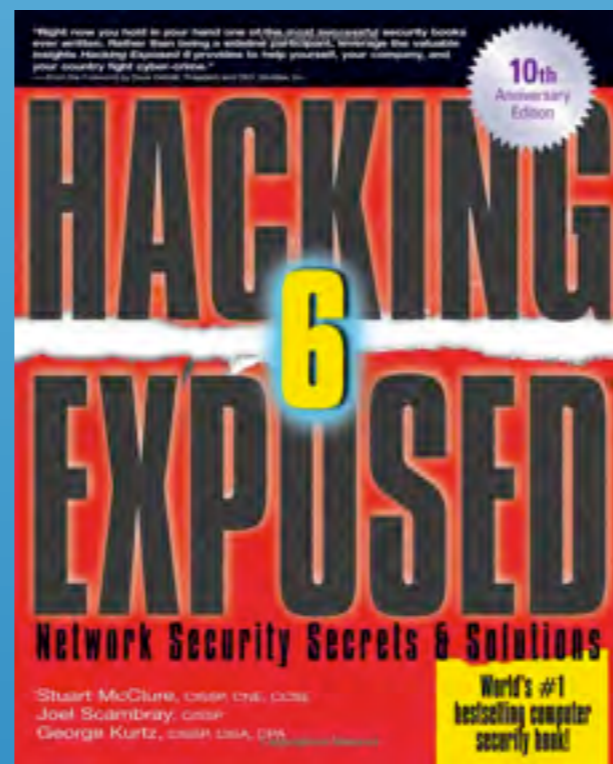
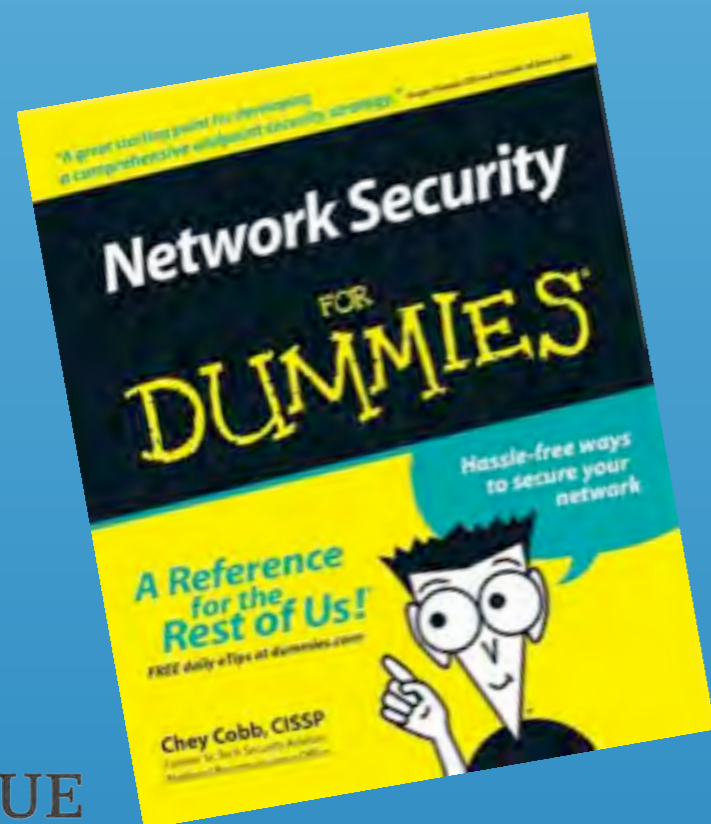
Characteristics of a Science

- Common, precisely defined terms.
- Standard references that everyone in the field knows and cites.
- Standard, independent units of measure.
- Science uses prior results and builds on known foundations.
- Predictive rather than reactive.

Common, precisely defined
terms?

Virus Spam Hack
Phishing Privacy
Cyberwar

Standard references that everyone in the field knows and cites?





Standard, independent
units of measure?

Standard, independent units of measure?

- What is a unit of confidentiality?

Standard, independent units of measure?

- What is a unit of confidentiality?
- How much privacy gain from quitting Facebook?

Standard, independent units of measure?

- What is a unit of confidentiality?
- How much privacy gain from quitting Facebook?
- If I delete a file, its confidentiality goes to 100% but availability goes to 0% — not independent.

Science uses prior results and builds on known foundations?

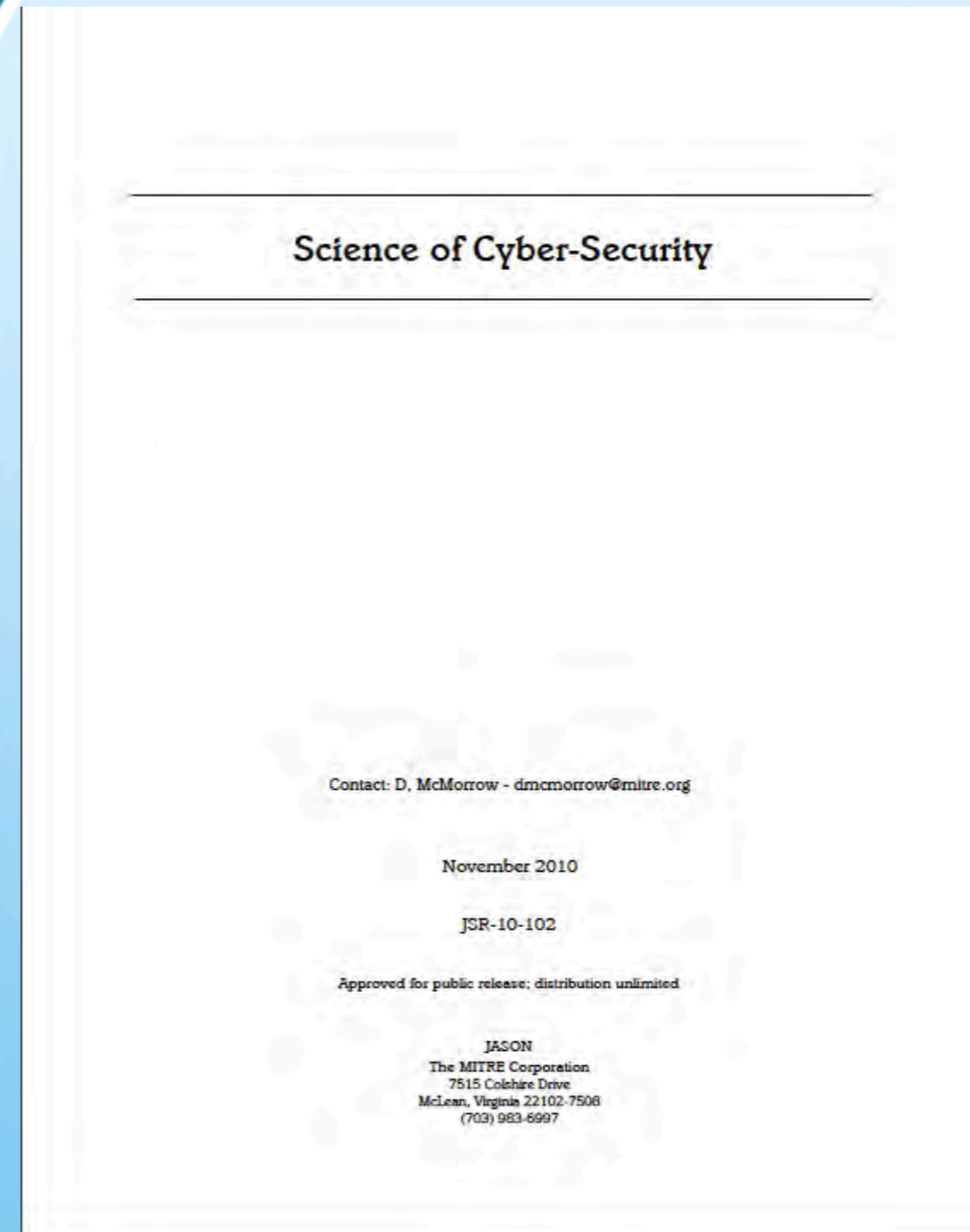
- 8000+ new vulnerabilities per year?
 - Buffer overflows — still? (identified in 1960s)
 - Weak passwords — still? (identified in 1950s)
- 2011 cellphones with viruses? (identified in 1980s)

Predictive rather than reactive?

- Culture of “penetrate and patch” is pervasive
- Common tools such as intrusion detection and data exfiltration are all reactive
- We don’t learn from the past, so never mind the future.

One View

- Focus on terms, but not principles or metrics.
- Bias towards model checking.
- (Typical) suggestion of large centers.
- Still focused on technology.





But what **is** Cyber Security?

What are the real challenges? How do we define the field?



Basic observation (Spaf's 1st Axiom of Cyber Security):



Basic observation

(Spaf's 1st Axiom of Cyber Security):

Without computers, we would have no cyber abuse.

And without people, we would have no cyber abuse.

Thus, focusing on the technology is only part of the solution.

We need to change the way we look at the field.

Cyber Security May Include

- Psychology
- Human factors
- Economics
- Education
- Risk management
- Organizational management
- Criminology
- Computer architecture
- Physical plant protection
- Disaster recovery/continuity
- ... and more

Example



- | | | | |
|-----------|-----------|-----------|----------|
| 1 | 123456 | 11 | Nicole |
| 2 | 12345 | 12 | Daniel |
| 3 | 123456789 | 13 | babygirl |
| 4 | Password | 14 | monkey |
| 5 | iloveyou | 15 | Jessica |
| 6 | princess | 16 | lovely |
| 7 | rockyou | 17 | Michael |
| 8 | 1234567 | 18 | Ashley |
| 9 | 12345678 | 19 | 654321 |
| 10 | abc123 | 20 | Qwerty |

Our systems were designed by experts — but for experts. We don't consider how novices view what we have built. No wonder they misuse it.

Need clear warnings



Inexpensive can be expensive



Antivirus XP 2008 demo mode notice

Antivirus XP 2008

ALERT This Computer is infected with spyware and adware

Spyware programs install keyloggers, steal credit card numbers and bank information details. This computer can be used for sending spam and you will get popups with adult content. If your homepage was changed or you have strange popups- this is a sure that your computer is infected

REGISTER Registration

We are strongly recommend you to register Antivirus XP 2008. You will get friendly 24/7/365 premium support, frequent updates and individual fixed from all known viruses!

NOT ACTIVE Virus Protection

Windows did not find any registered Antivirus XP 2008 software on this computer. Antivirus XP 2008 helps protect your computer against viruses and other security threats. Click Recommendations for suggested actions you can take.

Recommendations

Antivirus XP 2008

Continue unprotected [Click here to switch to the Full Mode.](#)

And not everything is Security

- About those 8000+ flaws per year...
- Those are only the *security-related* flaws. How about all the *other* flaws in the software?
- Software engineering is the field to address this issue.

So, what else?

- Most physical sciences have observable constants and phenomena. What would be the equivalent of Planck's constant, or Avogadro's number?
- Most social sciences use stochastic methods on semi-static entities. Cyber changes too quickly.
- Much of what happens depends on human intent.

Thus, it isn't obvious that there can be a true science of cyber security. But we can certainly do better.

Takeaway #1

There is a limit to how much we can improve our defenses simply by developing technology.

- The technology will be used by humans: humans who are uninformed, in a hurry, tired, clumsy, and make mistakes.
- The technology will also be used by humans who intend to circumvent, misuse and abuse it.

Takeaway #2

We have a lot to do to formalize and mature the field of cyber security.

- We can start by requiring at least basic scientific rigor in research.
- We need to stop being sloppy with our terminology.
- We can start asking that results be replicated, and negative results be shared.

Takeaway #3

We should think carefully about what basic cyber security properties are, and how to measure them.

- The traditional *Confidentiality, Integrity, Availability* model doesn't fit the bill.
- We will need to consider human factors and economics issues as components.

Takeaway #4

Cyber Security is not independent of other aspects of computing.

- We need to improve our software engineering, our operating systems, our human factors, our network protocols, ...
- This has implications for education in the field, too.

Takeaway #5

Cyber Security is not independent of other aspects of society.

- Pure defense is never enough. We need to improve our methods of investigation and prosecution to stop offenders and discourage abuse.
- We need to understand that our computing is used in places and cultures different from our own, and by people different than us.

Takeaway #6

If we aren't willing to make a significant investment to start from new foundations, it is certain that things will get worse.

- We are using artifacts we don't completely understand, purchased because of cost concerns, often developed in haste, with characteristics we can't measure, and a long history of flaws. This will not end well.



Thank

You!