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

PURDUE UNIVERSITY

The Environment

PURDUE
UNIVERSITY

The Environment

PURDUE
UNIVERSITY

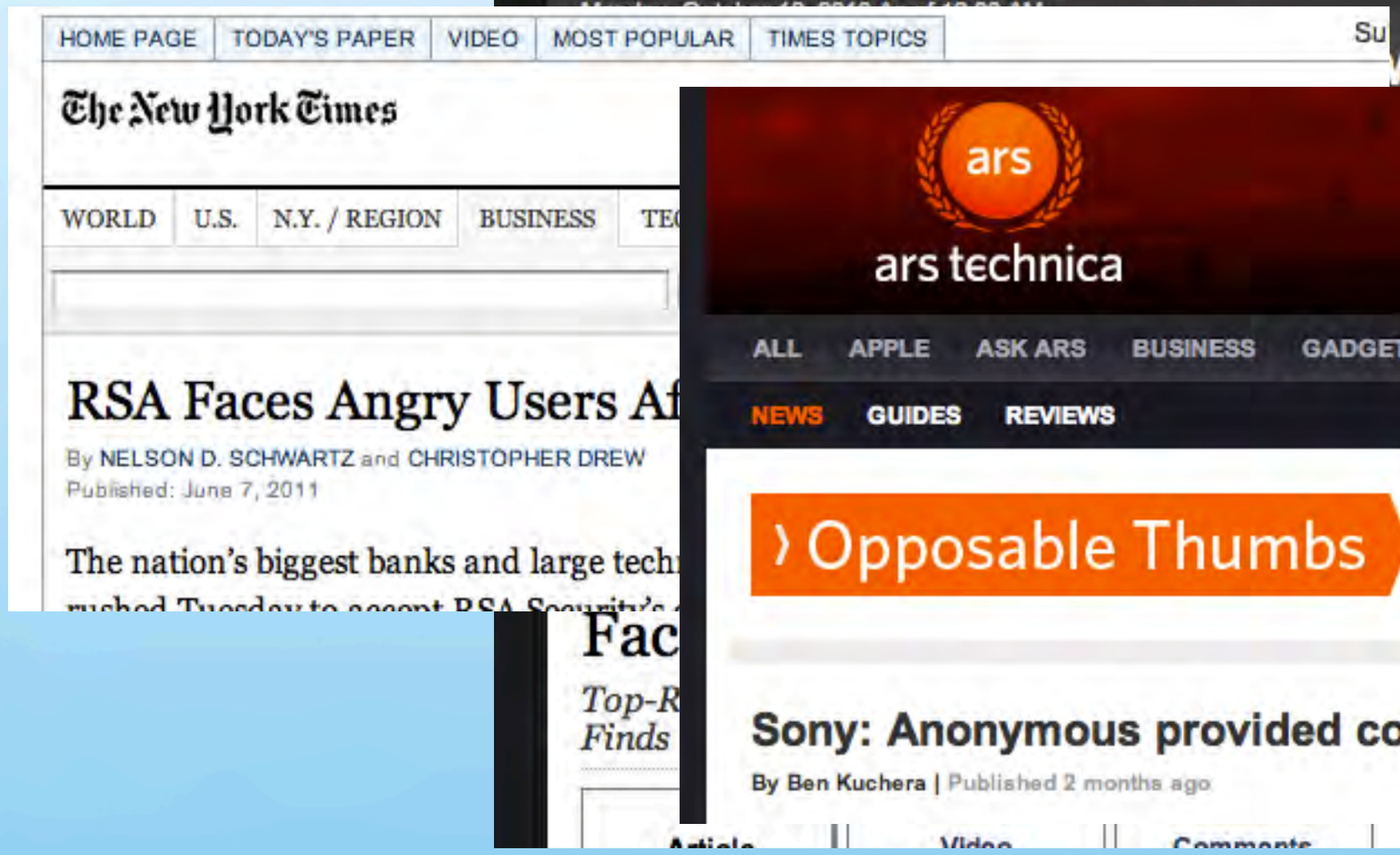
The Environment

PURDUE
UNIVERSITY

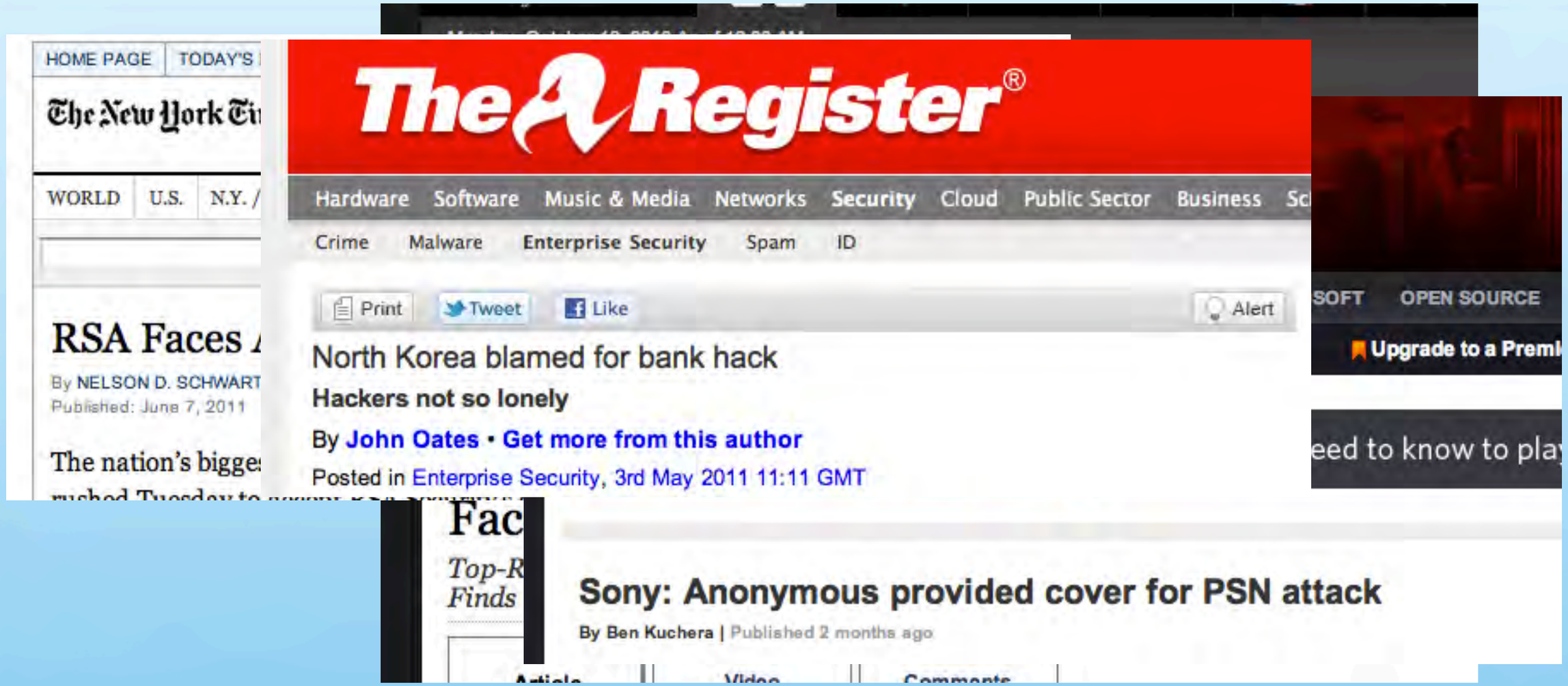
The Environment

PURDUE
UNIVERSITY

The Environment



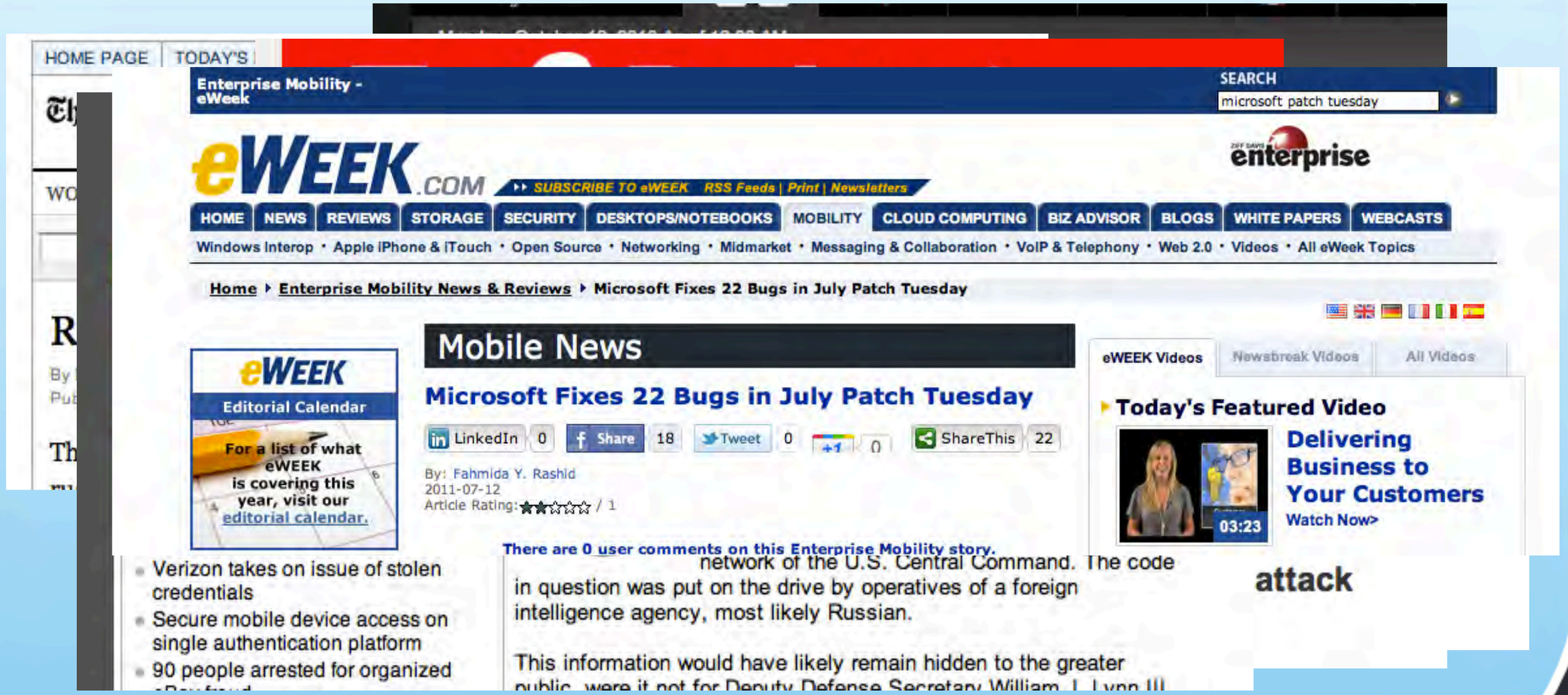
The Environment



The Environment

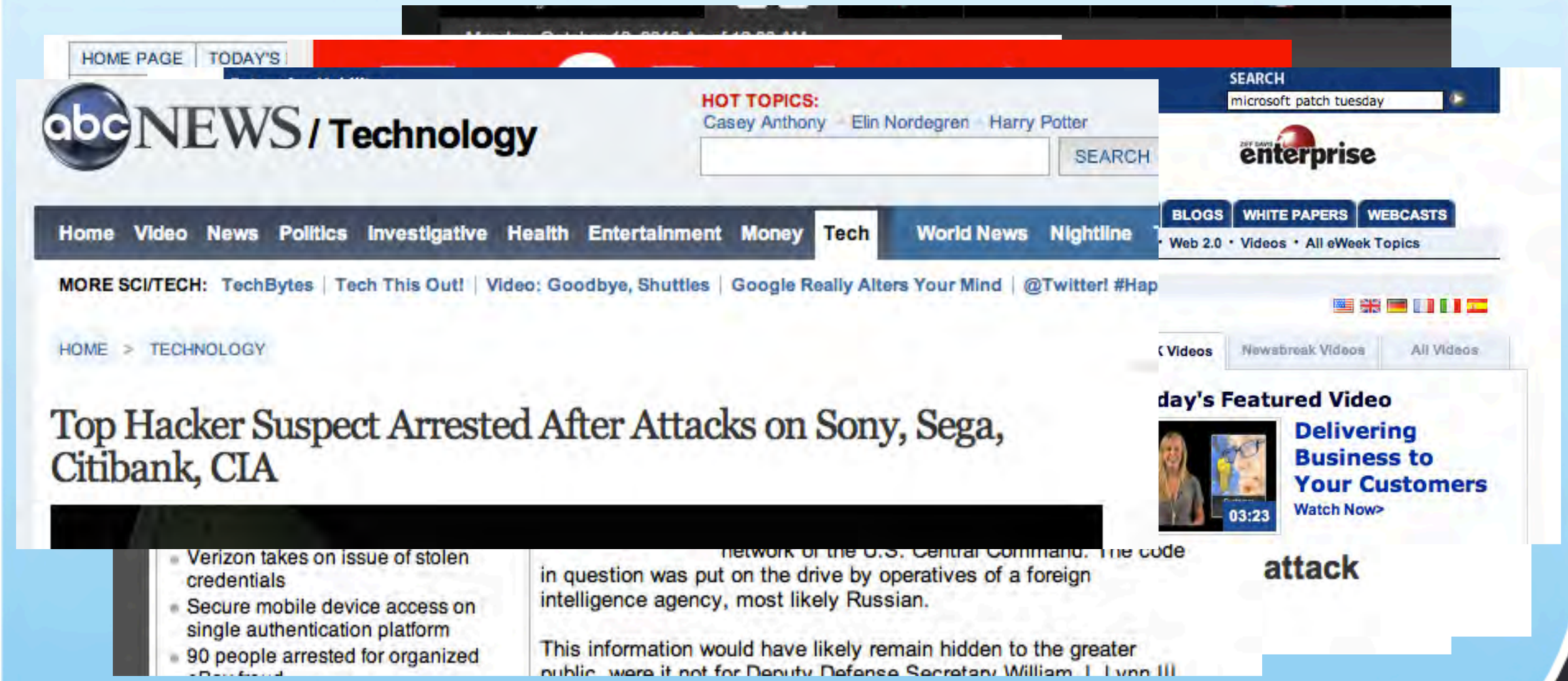
PURDUE
UNIVERSITY

The Environment



PURDUE UNIVERSITY

The Environment



PURDUE UNIVERSITY

The Environment

PURDUE
UNIVERSITY

The Environment

PURDUE
UNIVERSITY

The Environment

PURDUE UNIVERSITY

The Environment

PURDUE UNIVERSITY

The Environment

And hundreds of other incidents this year alone.

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

PURDUE UNIVERSITY

The Magnitude

PURDUE UNIVERSITY

Sources: ISS, NIST, FBI, McAfee Corp.

The Magnitude

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

Sources: ISS, NIST, FBI, McAfee Corp.

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

PURDUE UNIVERSITY

Sources: ISS, NIST, FBI, McAfee Corp.

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

PURDUE UNIVERSITY

Sources: ISS, NIST, FBI, McAfee Corp.

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

PURDUE UNIVERSITY

Sources: ISS, NIST, FBI, McAfee Corp.

Sources: McAfee Corp.

- For 1st quarter 2011 malware

PURDUE UNIVERSITY

Sources: McAfee Corp.

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

PURDUE UNIVERSITY

Sources: McAfee Corp.

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

Sources: McAfee Corp.

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

PURDUE UNIVERSITY

Sources: McAfee Corp.

- 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

PURDUE UNIVERSITY

Sources: McAfee Corp.

- 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

PURDUE UNIVERSITY

Sources: McAfee Corp.

Sources: Privacy Rights Clearinghouse, McAfee Corp.

- So far in 2011

PURDUE UNIVERSITY

Sources: Privacy Rights Clearinghouse, McAfee Corp.

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

PURDUE UNIVERSITY

Sources: Privacy Rights Clearinghouse, McAfee Corp.

- 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.

PURDUE UNIVERSITY

Sources: Privacy Rights Clearinghouse, McAfee Corp.

- 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.

PURDUE UNIVERSITY

Sources: Privacy Rights Clearinghouse, McAfee Corp.

- 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.

PURDUE UNIVERSITY

Sources: Privacy Rights Clearinghouse, McAfee Corp.

Clearly, there is a problem

Sources: U.S. Department of Commerce

Clearly, there is a problem

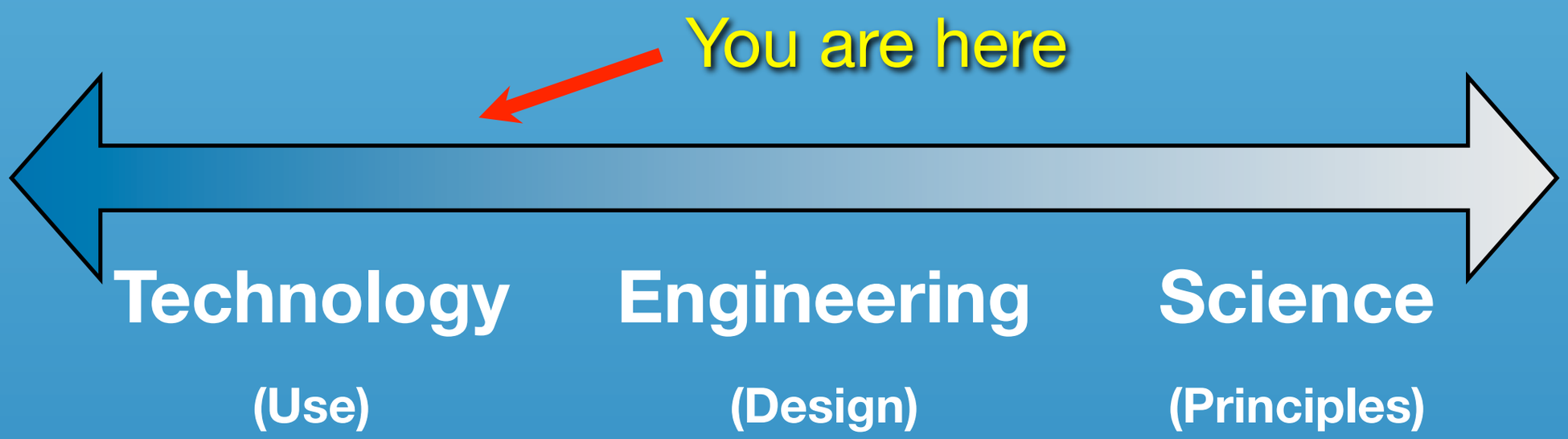
- But it isn't new!
- Some of us have been sounding the alarm for over 20 years.
- Spending on cyber security in the U.S. alone exceeds $8 billion a year but we are still falling behind.

PURDUE UNIVERSITY

Sources: U.S. Department of Commerce

One contention

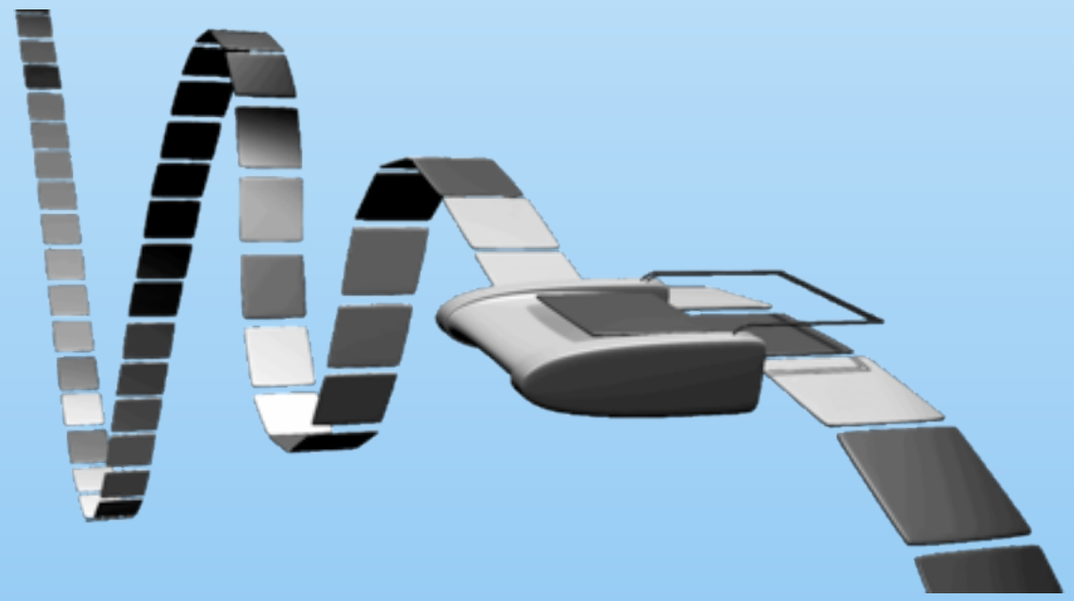
Our approach has been based on *ad hoc* practice rather than formal science



PURDUE UNIVERSITY

Hey, we do science! …don't we?

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



PURDUE UNIVERSITY

CERIAS

PURDUE
UNIVERSITY

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

PURDUE UNIVERSITY

When did you last see negative results published?

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

PURDUE UNIVERSITY

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

PURDUE UNIVERSITY

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.

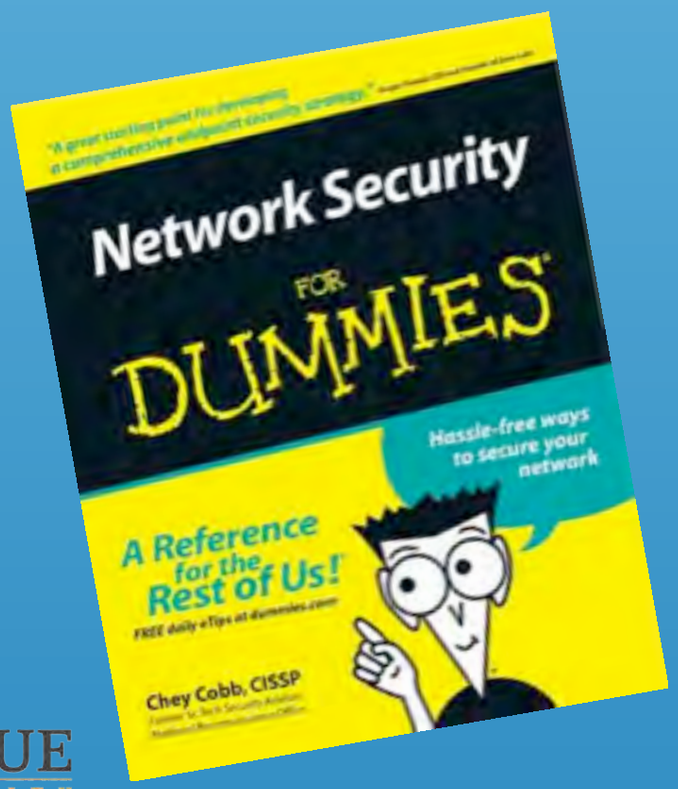
PURDUE UNIVERSITY

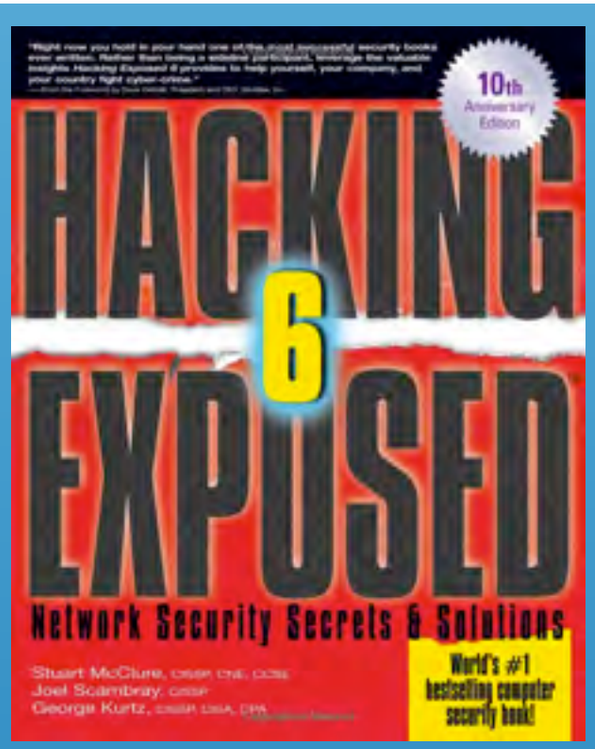
Common, precisely defined terms?

Virus Spam Hack
Phishing Privacy
Cyberwar

PURDUE UNIVERSITY

Standard references that everyone in the field knows and cites?





PURDUE UNIVERSITY

Standard, independent units of measure?

PURDUE
UNIVERSITY

Standard, independent units of measure?

- What is a unit of confidentiality?

PURDUE UNIVERSITY

Standard, independent units of measure?

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

PURDUE UNIVERSITY

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.

PURDUE UNIVERSITY

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)

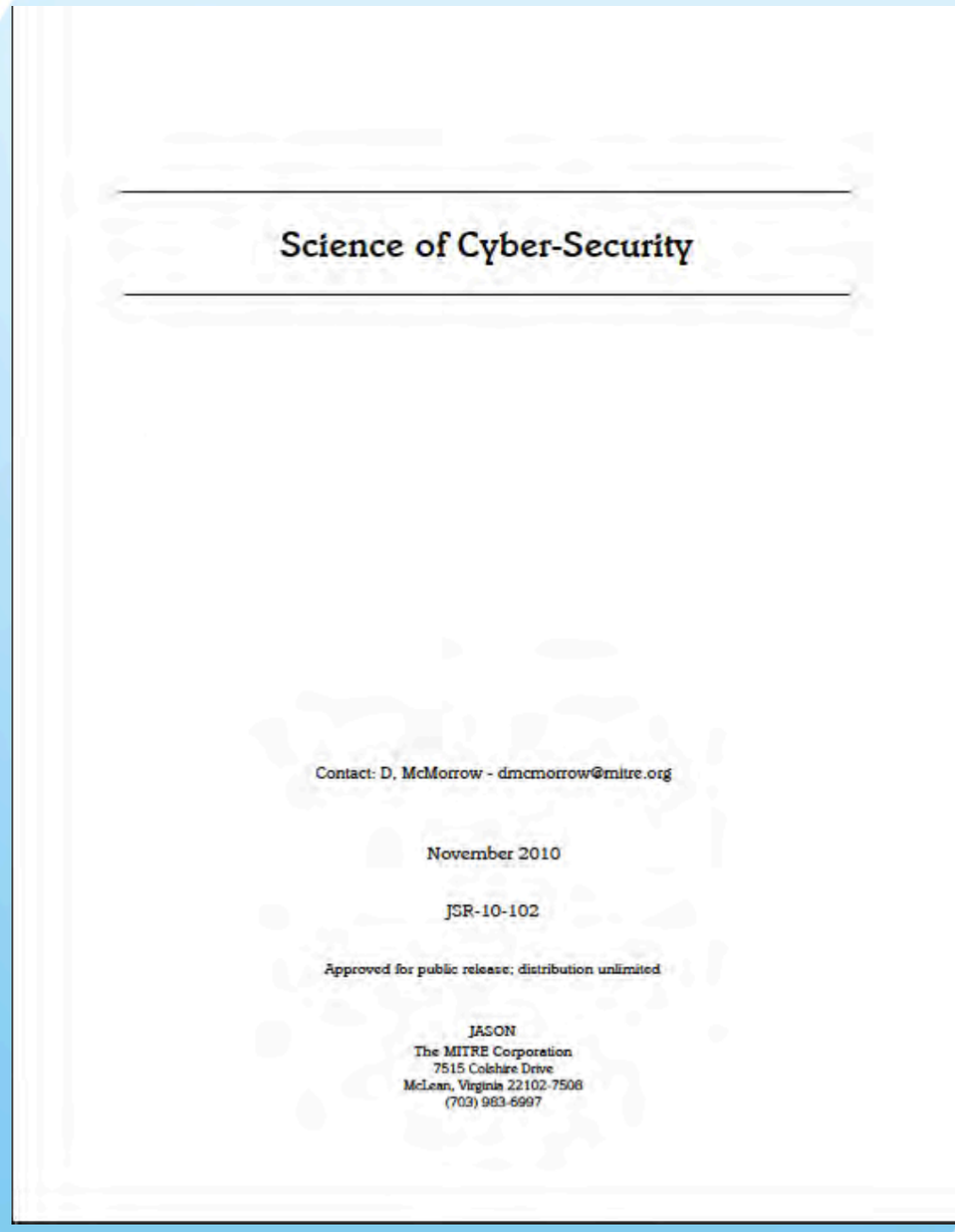
PURDUE UNIVERSITY

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.



Science of Cyber-Security

Contact: D. McMorrow - dmcmorrow@mitre.org

November 2010

JSR-10-102

Approved for public release; distribution unlimited

JASON
The MITRE Corporation
7515 Colshire Drive
McLean, Virginia 22102-7508
(703) 983-6997

PURDUE UNIVERSITY

But what **is** Cyber Security?

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

PURDUE UNIVERSITY

Basic observation

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

PURDUE
UNIVERSITY

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.

PURDUE UNIVERSITY

Cyber Security May Include

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

PURDUE UNIVERSITY

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.

PURDUE UNIVERSITY

Need clear warnings

PURDUE UNIVERSITY

Inexpensive can be expensive

PURDUE UNIVERSITY

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.

PURDUE UNIVERSITY

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.

PURDUE UNIVERSITY

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.

PURDUE UNIVERSITY

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.

PURDUE UNIVERSITY

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.

PURDUE UNIVERSITY

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.

PURDUE UNIVERSITY

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.

PURDUE UNIVERSITY

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.

PURDUE UNIVERSITY

Thank

You!

PURDUE
UNIVERSITY