Software Security

Pr. Dr. Yves ROUDIER
I3S – CNRS – UCA

Yves.Roudier@univ-cotedazur.fr

Software Security

- This is an introductory class about software security
  - High-level concepts
  - Hands-on experience on some attacks
  - Protection approaches
- We will also consider network and hardware security to some extent
  - Software is distributed, mobile, or embedded today.
- Now that you know how to write code, we will see how to break it, then how to secure it!
  - Understand software vulnerabilities
  - Security requirements engineering
  - Security architectures and countermeasures
  - Basic cryptography
  - Secure programming

A word of warning

- Don’t do this on others’ systems!
- Don’t do this on Polytech systems …
- Don’t do this in the wild neither for fun nor profit!

- Hacking/Cracking is illegal (and often unethical)
- This course discusses vulnerabilities in order to make you aware of the attack vectors that must be countered to secure software

- … you’ve been warned !!!!

- ***Le contenu de cet enseignement a un objectif strictement pédagogique. Toute personne utilisant son contenu hors de ce cadre s’expose à rendre des comptes devant des juridiques !***

Developing your security awareness

- **Theory:** how the attacks work, what are software protection principles and mechanisms, etc.
- **Practice:** run a few attacks, manipulate security libraries and tools for security testing, write secure code or deploy countermeasure
- **Mindset:** learn to think as an attacker, not just as a developer : you need to understand how to break a system before being able to create a secure design

(Tentative) Course Outline

- Malware and Attacks: an Introduction
- Software Exploits 1: Web Apps
- Software Exploits 2: Low level attacks
- Basic Cryptography
- Secure Software Development Life-Cycle
- Secure Programming
- Enpoint Detection and Response
- Basic Pentesting / Security testing

About the course

- Slides and labs: available on the LMS Moodle (Software Security - EIEISE7)
  - WHEN the administration will have created the Moodle repository !!!
  - I will be using the Slack channel in between …
- Grading
  - Quizzes and homeworks (20%)
    - questions and exercises about course and labs
  - Research paper study (30%)
    - Video presentation by groups of 3-4 students
  - Secure Programming project (50%)
    - Software development using a secure programming approach
- Labs will NOT be graded
  - No need to turn in a report
- Communications : get in touch through
  - Slack (#si4-softsec or DM)
  - email Yves.Roudier@univ-cotedazur.fr (especially if this requires some work from my side)

After this course …

- CyberSec minor
  - SI5 / Master 2 (Apprenticeship)
- Security Courses:
  - Cryptographie et Sécurité
  - Cybersécurité
  - Security and Privacy 3.0
  - Sécurité dans les réseaux
  - Sécurité des applications web
  - Security for IoT, CPS and embedded systems

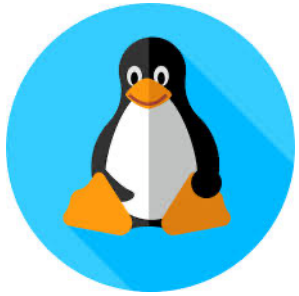
Security: Why should you care?

- Security impacts on our daily lives
- Become a security-aware user
  - Make wise and informed decision when using software and computer systems
- Become a security-aware developer or security consultant
  - Design and build secure software and systems, pentest systems, etc.
- Become a security researcher
  - Discover unknown security flaws and/or propose original solutions

Security is hard to capture

- Network Security
  - Perimeter protection (authentication & more)
  - Protecting communications
- System Security
  - Security policies (Rights management, access control/usage)
- Hardware Security
  - Physical attacks over processors and memory
- Software Security
  - Software Vulnerabilities
  - Information flow protection
  - IPR protection (obfuscation, fingerprinting …)

Software is everywhere (everyware?)



Operating Systems

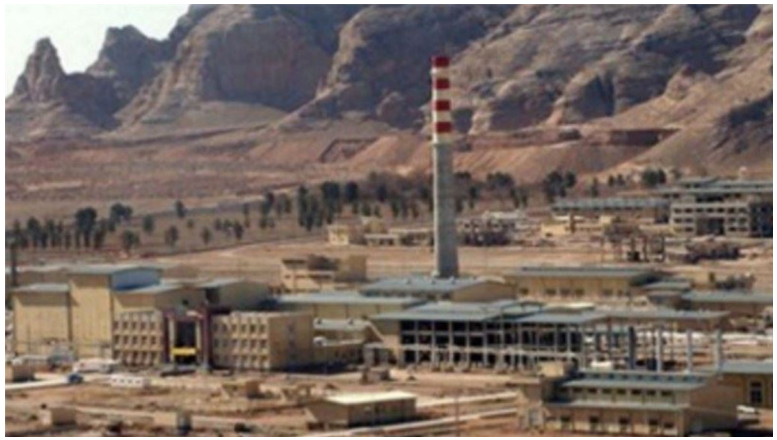
Native Applications

Web Applications

Software is everywhere (everyware?)

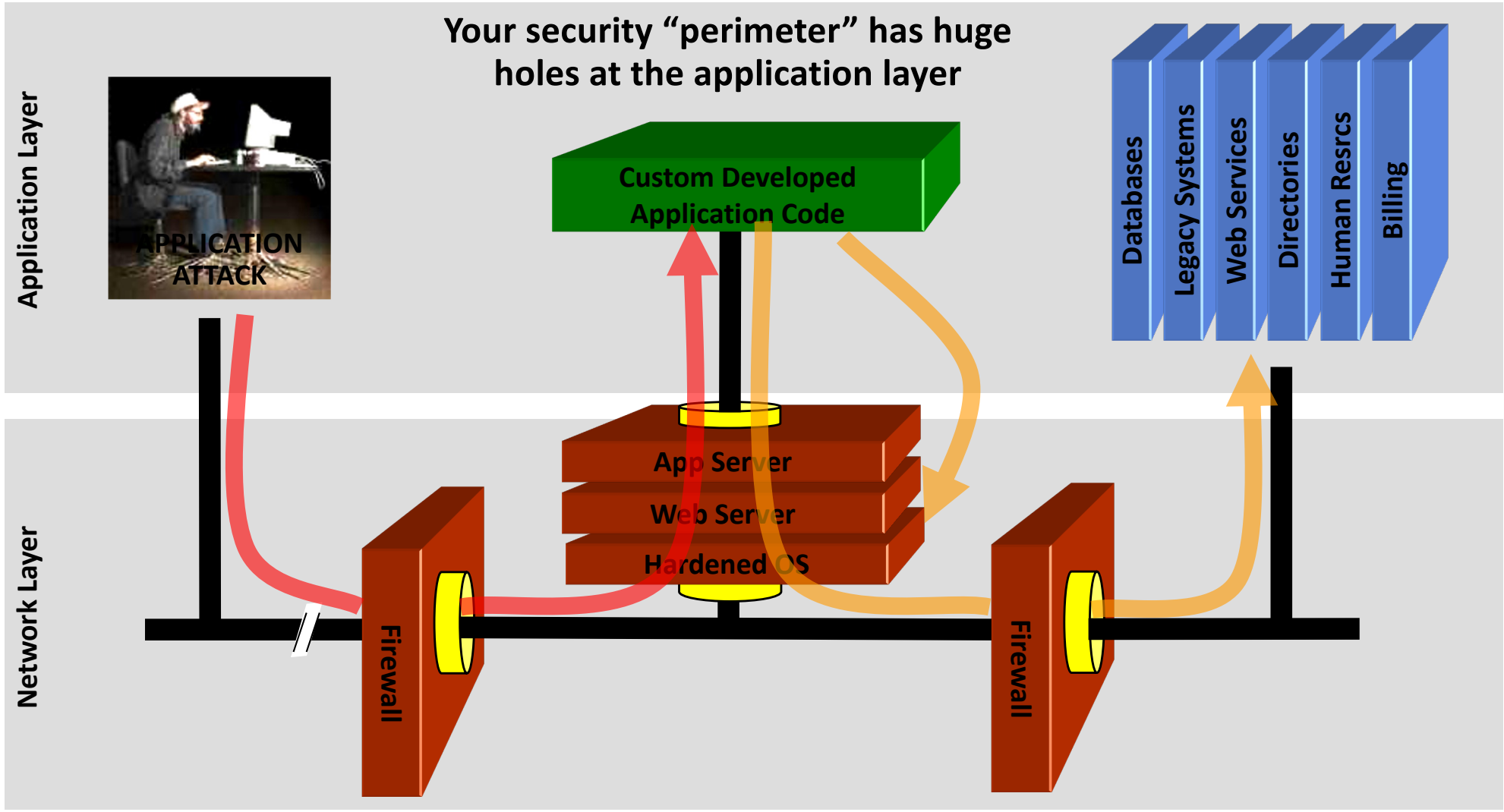
Network stacks

Security systems (smartcards, firewalls)



Cyber-Physical Systems (IoT, vehicles, plants)

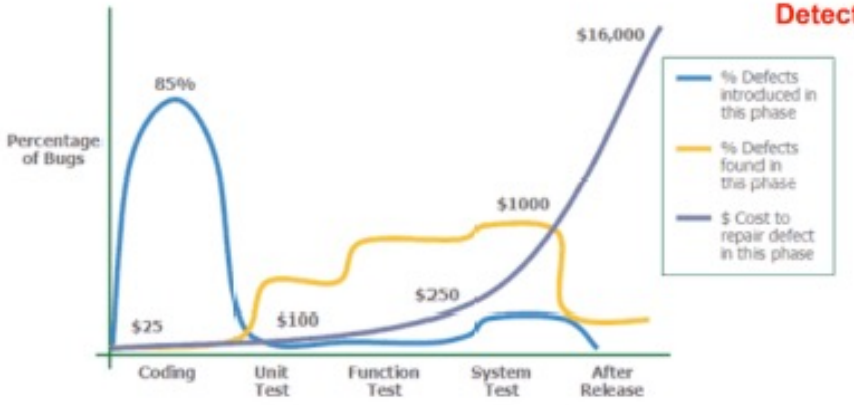
Blurred Lines: Your Code is Part of Your Security Perimeter



You can't use network layer protection (firewall, SSL, IDS, hardening) to stop or detect application layer attacks

Software and Security Engineering

- Multiple actors
- Separation of responsabilities
- Secure SDLC



"applied software measurement"
Capers Jones 1996

Vulnerable Software

- Computer systems still have many vulnerabilities
  - Vocabulary: Human error -> fault (bug or unwanted access) -> security failure (vulnerability) -> exploitation (compromise)
- Technical factors
  - It's complex!
  - Wrong configuration vs. logical faults
- Organizational factors
  - Security = cost center!
  - Deadline pressure
- Human factors
  - Designer mindset
  - Environment

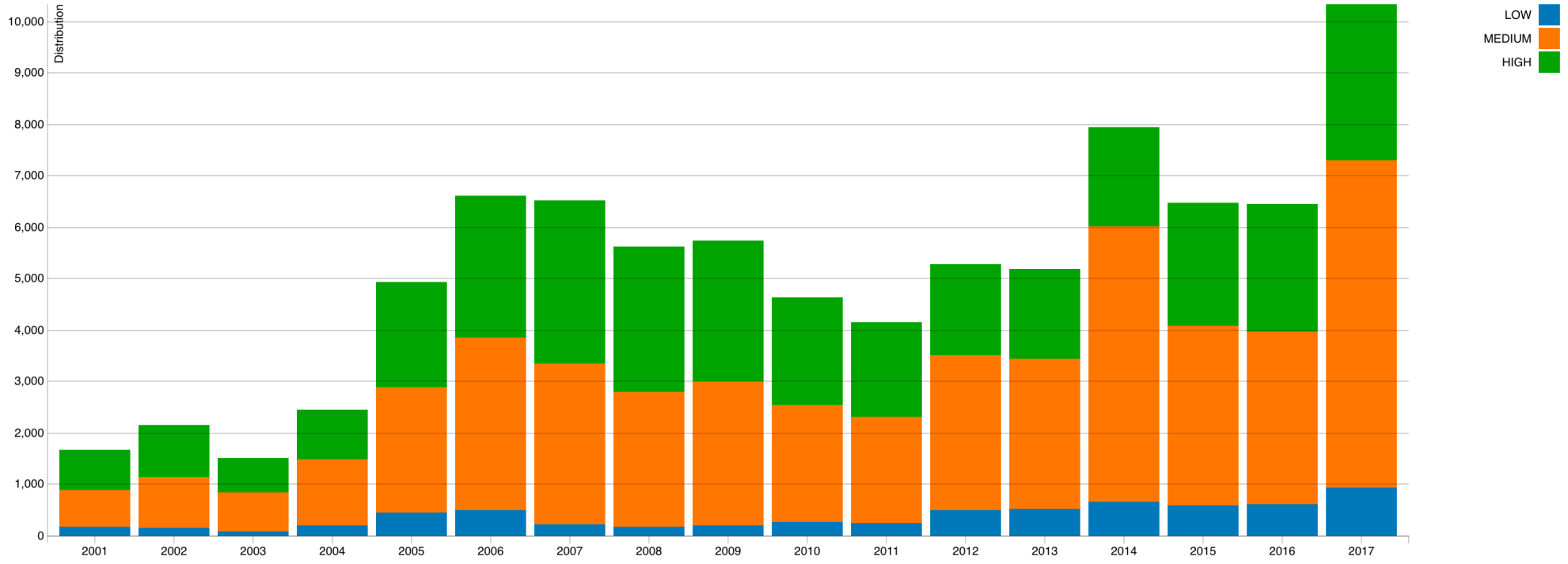
Bruce Schneier's law (according to Cory Doctorow): "Any person can invent a security system so clever that he or she can't imagine a way of breaking it."

Vulnerable Software

- Exploitation is as old as remote access
  - Major issue as computer systems become more ubiquitous
  - Exposure to remote access (e.g. the Internet) leads to exploitation
  - 1973 - Bob Metcalfe's *RFC 602: "The Stockings Were Hung by the Chimney with Care" (about security issues in the ARPANET)*
    - "Many people still use passwords which are easy to guess: their first names, their initials, their host name spelled backwards, a string of characters which are easy to type in sequence"

Software Flaws

https://web.nvd.nist.gov/view/vuln/statistics



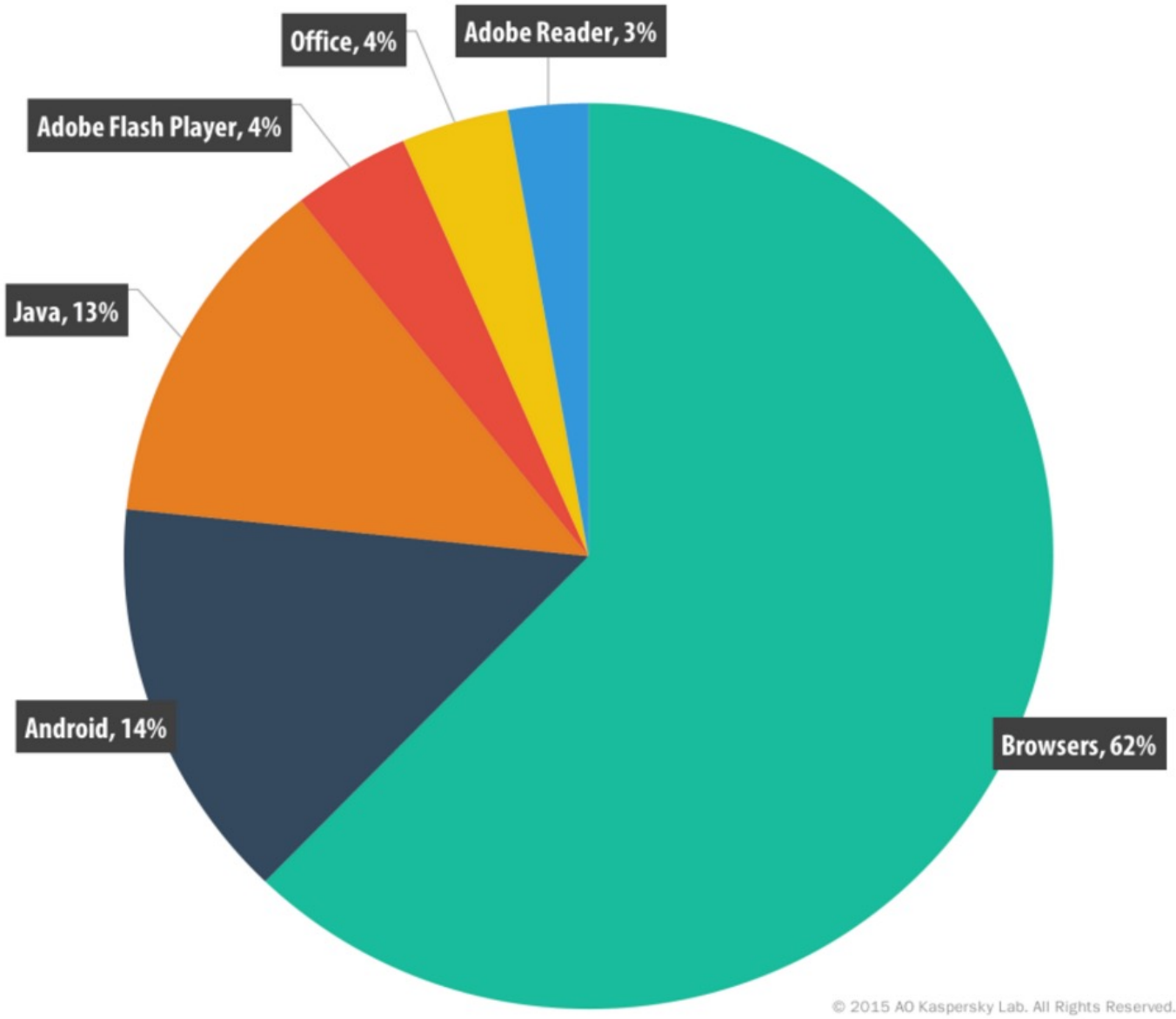
- CVSS Severity Distribution Over Time

Vulnerability disclosures (2015)

	Product Name	Vendor Name	Product Type	Number of Vulnerabilities
1	Mac Os X	Apple	OS	385
2	Iphone Os	Apple	OS	376
3	Flash Player	Adobe	Application	313
4	Air Sdk	Adobe	Application	246
5	AIR	Adobe	Application	246
6	Air Sdk & Compiler	Adobe	Application	246
7	Internet Explorer	Microsoft	Application	231
8	Chrome	Google	Application	187
9	Firefox	Mozilla	Application	178
10	Windows Server 2012	Microsoft	OS	155
11	Ubuntu Linux	Canonical	OS	152
12	Windows 8.1	Microsoft	OS	151

source: www.cvedetails.com/top-50-products.php?year=2015

Vulnerable applications being exploited



Source: Kaspersky Security Bulletin 2015

A few references

- Books:
  - Gildas Avoine, Pascal Junod, Philippe Oechslin, Sylvain Pasini. Sécurité informatique, Cours et exercices corrigés. Vuibert.
  - Ross Anderson. Security Engineering. Wiley. (http://www.cl.cam.ac.uk/~rja14/book.html)
- Conferences:
  - Academic: Security&Privacy (Oakland), CCS, Usenix Security, NDSS, ESORICS, RAID, ACSAC, DSN
  - Non-academic: DefCon, BlackHat, SSTIC, GreHack