Ethical Hacking / Penetration testing Network Security

Boldizsár Bencsáth PhD

When ‘ OR 1=1 -- works

BTK 423

- **Információs rendszer vagy adat megsértése**
- **423. §** (1) Aki
- *a)* információs rendszerbe az információs rendszer védelmét biztosító technikai intézkedés megsértésével vagy kijátszásával jogosulatlanul belép, vagy a belépési jogosultsága kereteit túllépve vagy azt megsértve bent marad,
- *b)* az információs rendszer működését jogosulatlanul vagy jogosultsága kereteit megsértve akadályozza, vagy
- *c)* információs rendszerben lévő adatot jogosulatlanul vagy jogosultsága kereteit megsértve megváltoztat, töröl vagy hozzáférhetetlenné tesz,
- vétség miatt két évig terjedő szabadságvesztéssel büntetendő.
- (2) A büntetés bűntett miatt egy évtől öt évig terjedő szabadságvesztés, ha az (1) bekezdés *b)-c)* pontjában meghatározott bűncselekmény jelentős számú információs rendszert érint.
- (3) A büntetés két évtől nyolc évig terjedő szabadságvesztés, ha a bűncselekményt közérdekű üzem ellen követik el.
- (4) E § alkalmazásában adat: információs rendszerben tárolt, kezelt, feldolgozott vagy továbbított tények, információk vagy fogalmak minden olyan formában való megjelenése, amely információs rendszer általi feldolgozásra alkalmas, ideértve azon programot is, amely valamely funkciónak az információs rendszer által való végrehajtását biztosítja.

BTK 424

- **Információs rendszer védelmét biztosító technikai intézkedés kijátszása**
- **424. §** (1) Aki a 375. vagy a 423. §-ban meghatározott bűncselekmény elkövetése céljából az ehhez szükséges vagy ezt könnyítő
- *a)* jelszót vagy számítástechnikai programot készít, átad, hozzáférhetővé tesz, megszerez, vagy forgalomba hoz, illetve
- *b)* jelszó vagy számítástechnikai program készítésére vonatkozó gazdasági, műszaki, szervezési ismereteit más rendelkezésére bocsátja,
- vétség miatt két évig terjedő szabadságvesztéssel büntetendő.
- (2) Nem büntethető az (1) bekezdés *a)* pontjában meghatározott bűncselekmény elkövetője, ha - mielőtt a bűncselekmény elkövetéséhez szükséges vagy ezt megkönnyítő jelszó vagy számítástechnikai program készítése a büntető ügyekben eljáró hatóság tudomására jutott volna - tevékenységét a hatóság előtt felfedi, az elkészített dolgot a hatóságnak átadja, és lehetővé teszi a készítésben részt vevő más személy kilétének megállapítását.
- (3) E § alkalmazásában jelszó: az információs rendszerbe vagy annak egy részébe való belépést lehetővé tevő, számokból, betűkből, jelekből, biometrikus adatokból vagy ezek kombinációjából álló bármely azonosító.
- **XL**

Network hacking

- Computer systems are complex
- Networked systems are even more complex
- Complex things always contain weaknesses, vulnerabilities
- Hacking systems are possible because there are weaknesses, vulnerabilities, mistakes, errors, backdoor, misconfigurations, wrong things, dragons
- The systems can be cracked, because of the vulnerabilities, not because you have open ports, you have bad firewall, you don't have antivirus
- Hacking a system can be avoided by hardening OS (think grsecurity patch), but using firewalls, etc.
- But these don't fix the root cause: the vulnerabilities

Ok, we need to kill vulnerabilities

- Let's make tools to eliminate vulnerabilities automatically
- Let's make languages where buffer overflow is not a problem
- Don't accept weak passwords as these can be cracked

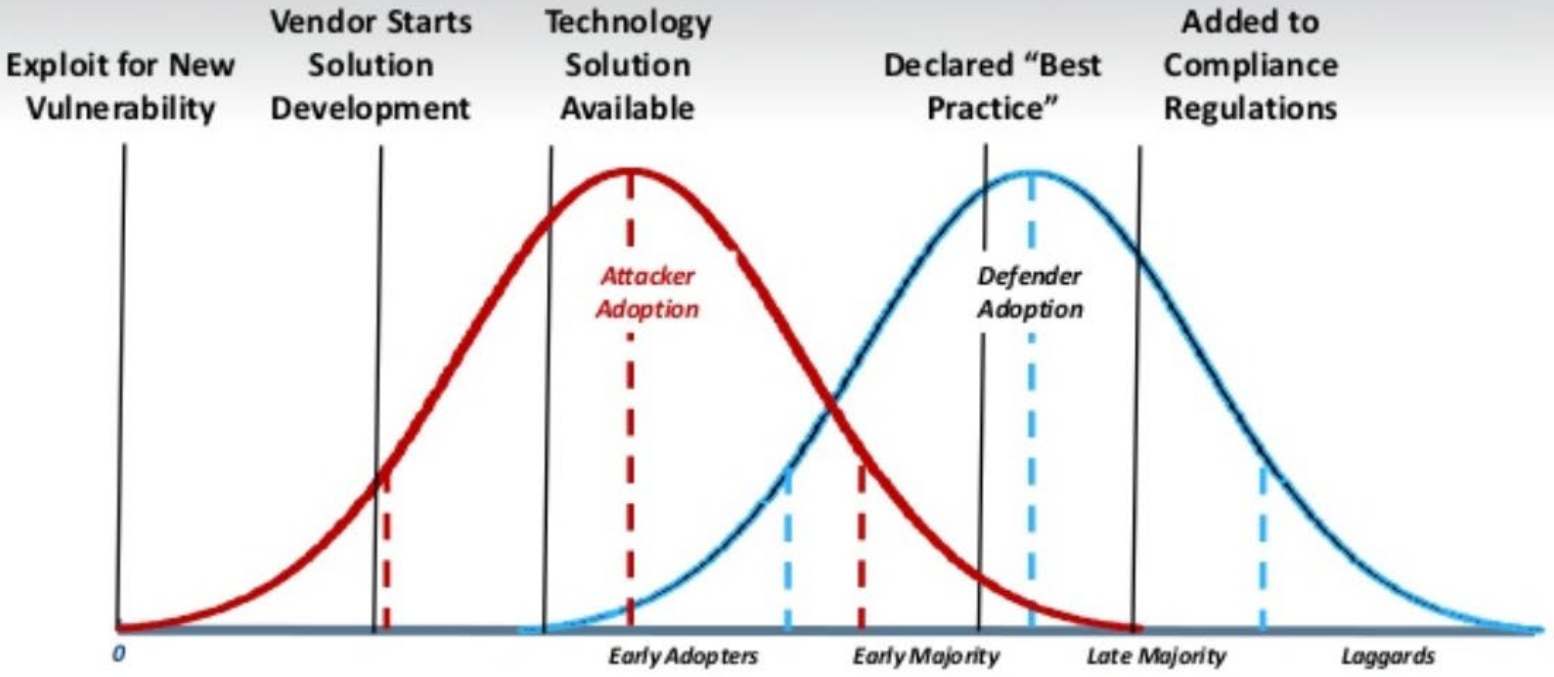
- No, all vulnerabilities cannot be eliminated
- No, it is sometimes impossible to find all vulnerabilities
  - Call flow graph is possibly insanely complex
  - Complexity of fuzzing can be insane (all possible inputs are enormously large)

Some very tough problems

- Race conditions: two or more different tasks can influence each others
- Interaction of different layers
  - E.g. Two systems understand the same data in different way
- Novel mathematical methods to crack crypto and such cannot be foreseen
- Side channel attacks (e.g. power, sound, etc.)
- Protection against DoS attacks
- Hardware problems, including CPU errata, timing attacks (e.g. see DDR raw hammer attack)

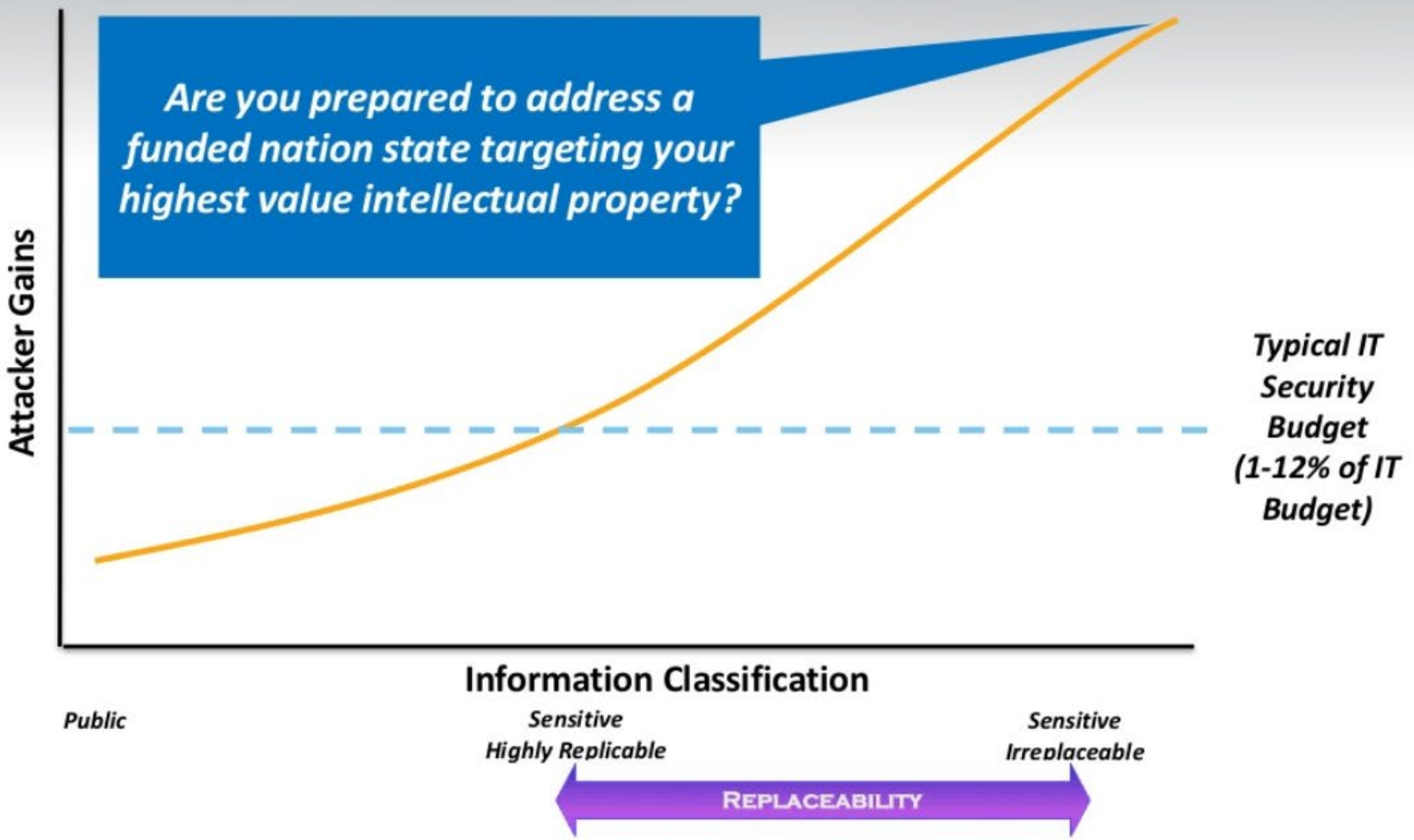
http://www.slideshare.net/DavidEtue/adversary-roi-evaluating-security-from-the-threat-actors-perspective

Solely Managing Vulnerabilities Will Never Win

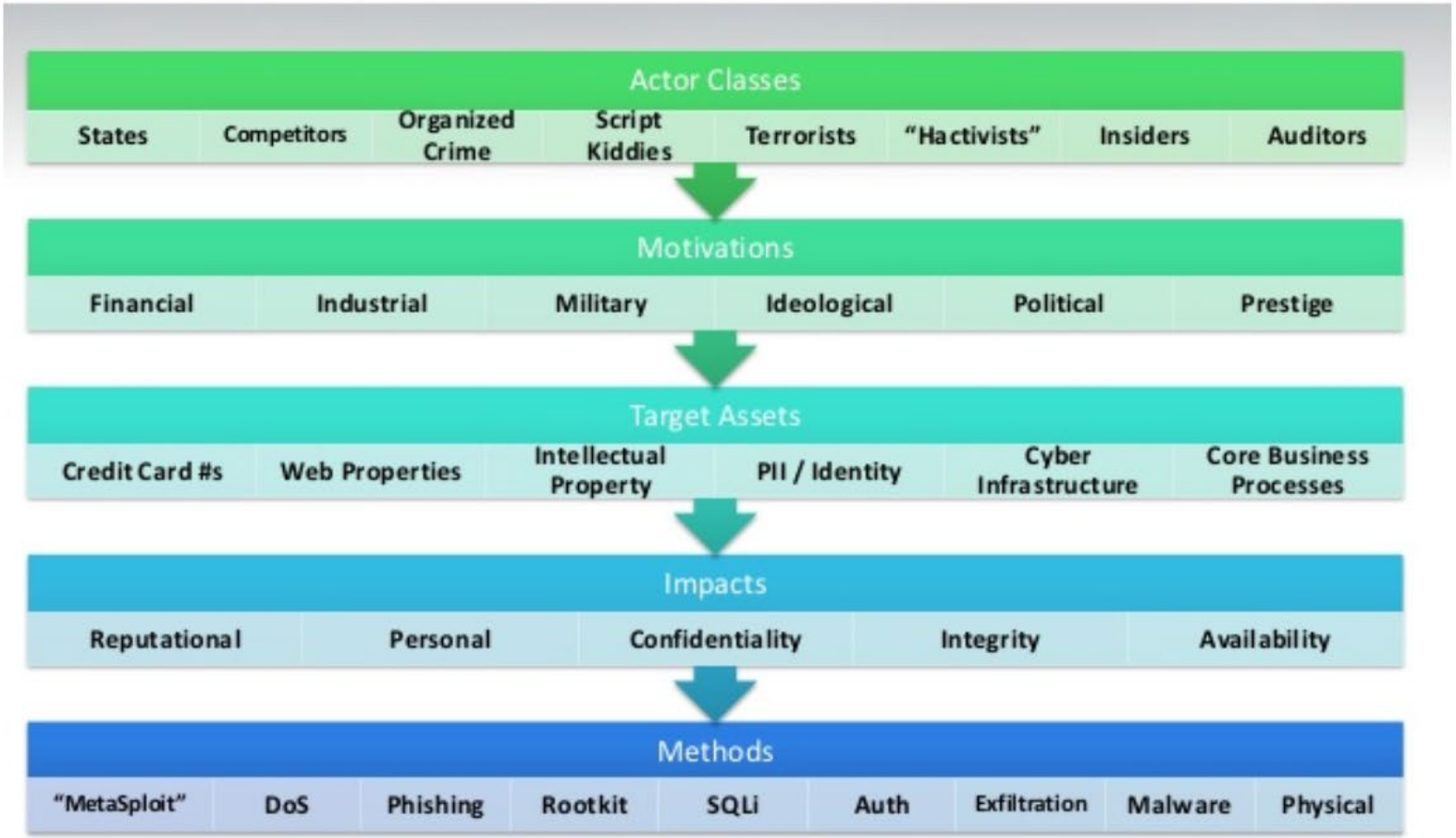


Extensive Lag Between Attack Innovation, Solution, and Adoption

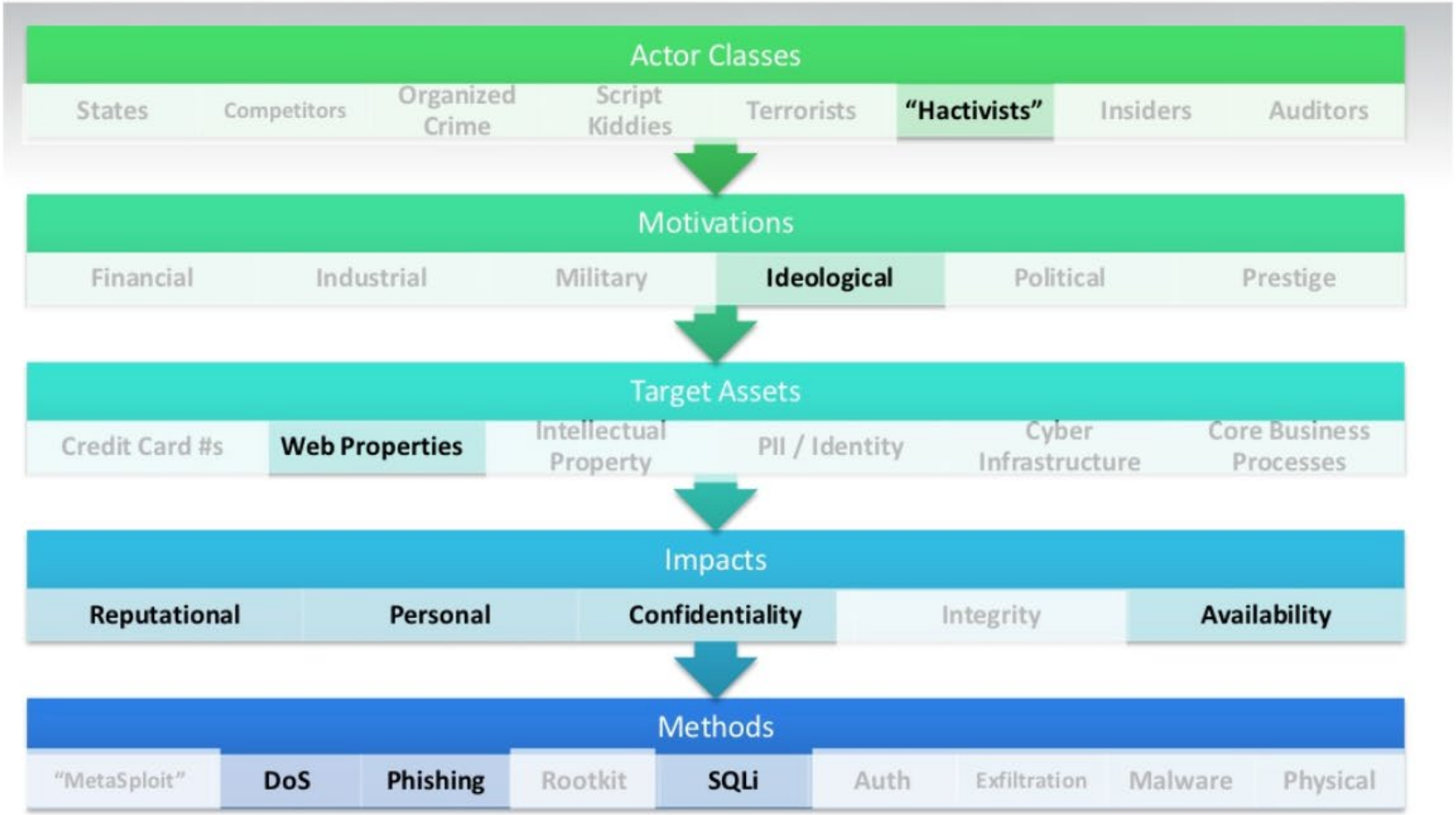
Value Favors the Attacker



A Modern Pantheon of Adversary Classes



Profiling a Particular Actor



Compare and Contrast Threat Actors

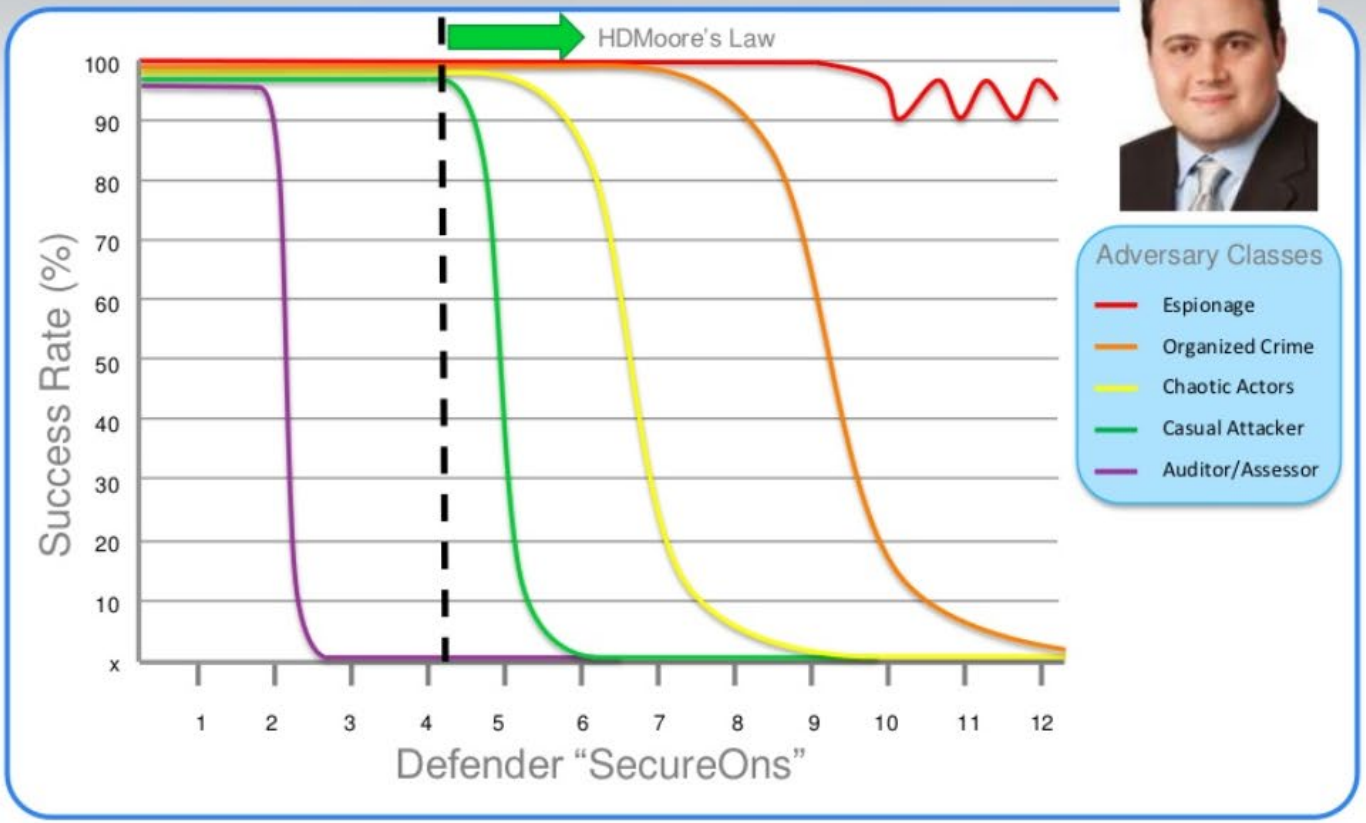
	QSA	Casual Attacker	Chaotic Actor	Org Crime	State APT/APA
Asset Focus	CCNs	CCNs…	Reputation, Dirty Laundry DDoS/Availability	CCNs Banking Fungible $	IP, Trade Secrets, National Security Data
Timeframe	Annual	Anytime	Flash Mobs	Continuous	Long Cons
Target Stickiness	NA	LOW	HIGH	LOW	HIGH
Probability	100%	MED	?	HIGH	?
"Impact"	Annual $	1 and done	Relentless	Varies	Varies

Attacker Power - HD Moore's Law

- **Moore's Law:** Compute power doubles every 18 months
- **HDMoore's Law:** Casual Attacker Strength grows at the rate of MetaSploit

http://www.slideshare.net/DavidEtue/adversary-roi-evaluating-security-from-the-threat-actors-perspective

HDMoore's Law (continued)



http://blog.cognitivedissidents.com/2011/11/01/intro-to-hdmoores-law/

1. Security stakeholders

- Security chief (CIO, etc.)
- Owners/managers
- Employees
- Internet Service Provider
- Contracted professionals (security product vendors, ethical hackers, etc.)
- Auditors
- Outsider attackers

- Everybody has a different goal
- Everybody has different permissions, possibilities
- Something working in the classroom might not work in real-life

Attackers

- Internal attackers
- Script kiddies
- Internet-wide scans (botnets, worms, etc.)
- Targeted attackers (with low budget)
- Professional targeted attackers (high budget)

Differences:

- What tools can they use (budget, knowledge)
- What time constraint they have
- How much computing, network resources they have
- How targeted is the attack
- What (how deep, sophisticated) is the main goal of an attack (e.g. just have a proxy -> ransom, multi-million dollar theft, obtaining millions of credit cards)

Point-of-View of the attacker

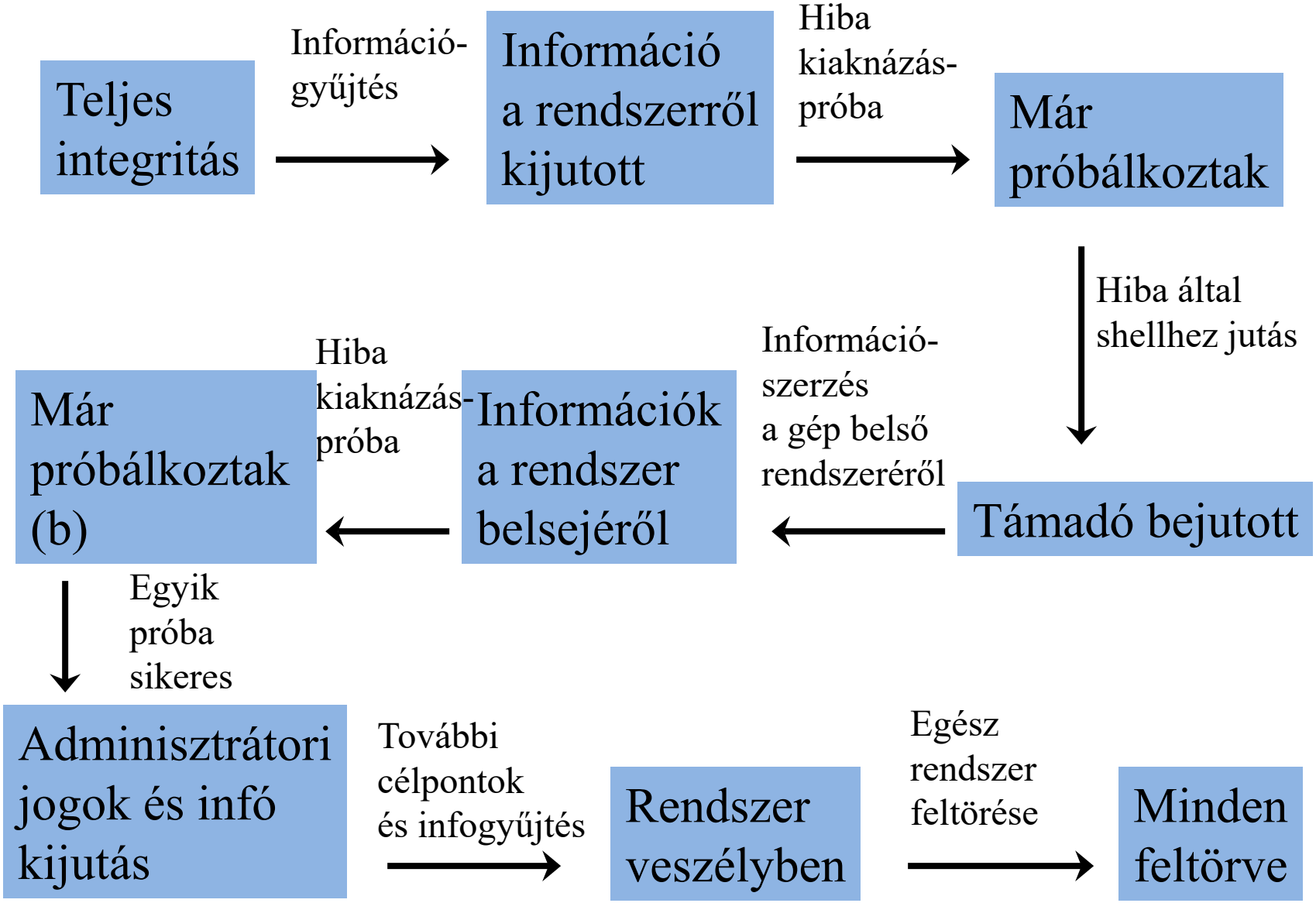
- The attacker focuses on errors rather than what is working
- Tries to find the weakest point
- Finds new ways to attack

This is why security testing, audits are important!

- If You learned security, You can avoid typical errors
- However, It is hard to identify system-wide problems at the first glance, during a large-scale development
- … And nobody has enough time to do everything in a secure fashion

It is not impossible to do security testing against Your own work – just take a different hat and a bit different thinking,…

How a typical hacker compromises a system



Simple attacks with high risk

- Internal attacker (employee) copies secret information before leaving company
- Social engineering: Employee gives credentials to attackers (e.g. phone call, dumpster diving)
  - Near impossible to avoid
- Passwords on stickers near the computer

- Sometimes these problems lead to higher risks than a missing update, a vulnerable kernel or a bad password
  (-> risk analysis is important!)

Dictionary – first words

- **Vulnerability** - a flaw or weakness in a system's design, implementation, or operation and management
- **Threat** - a possible way to exploit vulnerabilities
- **Attack** - a *deliberate attempt* to compromise a system
- **Exploit** - is a piece of software, a chunk of data, or sequence of commands that take advantage of a bug, glitch or vulnerability in order to cause unintended or unanticipated behavior to occur on computer Rootkit
- **Backdoor** - a method of bypassing normal authentication, securing remote access to a computer by an attacker
- **0-day** (zero day) (exploit) - a computer threat that tries to exploit computer application vulnerabilities that are unknown to others
- **DoS** – Denial of Service - an attempt to make a computer resource unavailable to its intended users
- **Spoofing** - a situation in which one person or program successfully masquerades as another by falsifying data

Security terms 2.

- **Sniffing** - intercepts and log traffic passing over a digital network
- **Scanner** – tries numerous hosts angainst a vulnerability or to find open services
- **Portscan** – only scans for open TCP/UDP ports of a system to identify potential targets
- **Fingerprinting** – find characteristic information of a system or tool, e.g. find out what operating system is in use, or what tool has been used.
- **Cracker** - a Black-hat computer hacker, a person who breaks security
- **Hacker** - who makes innovative customizations or combinations of retail electronic and computer equipment (but often used as a synonym of cracker)
- **Ethical hacker** - computer security experts, who specialize in penetration testing, and other testing methodologies, to ensure that a company's information systems are secure

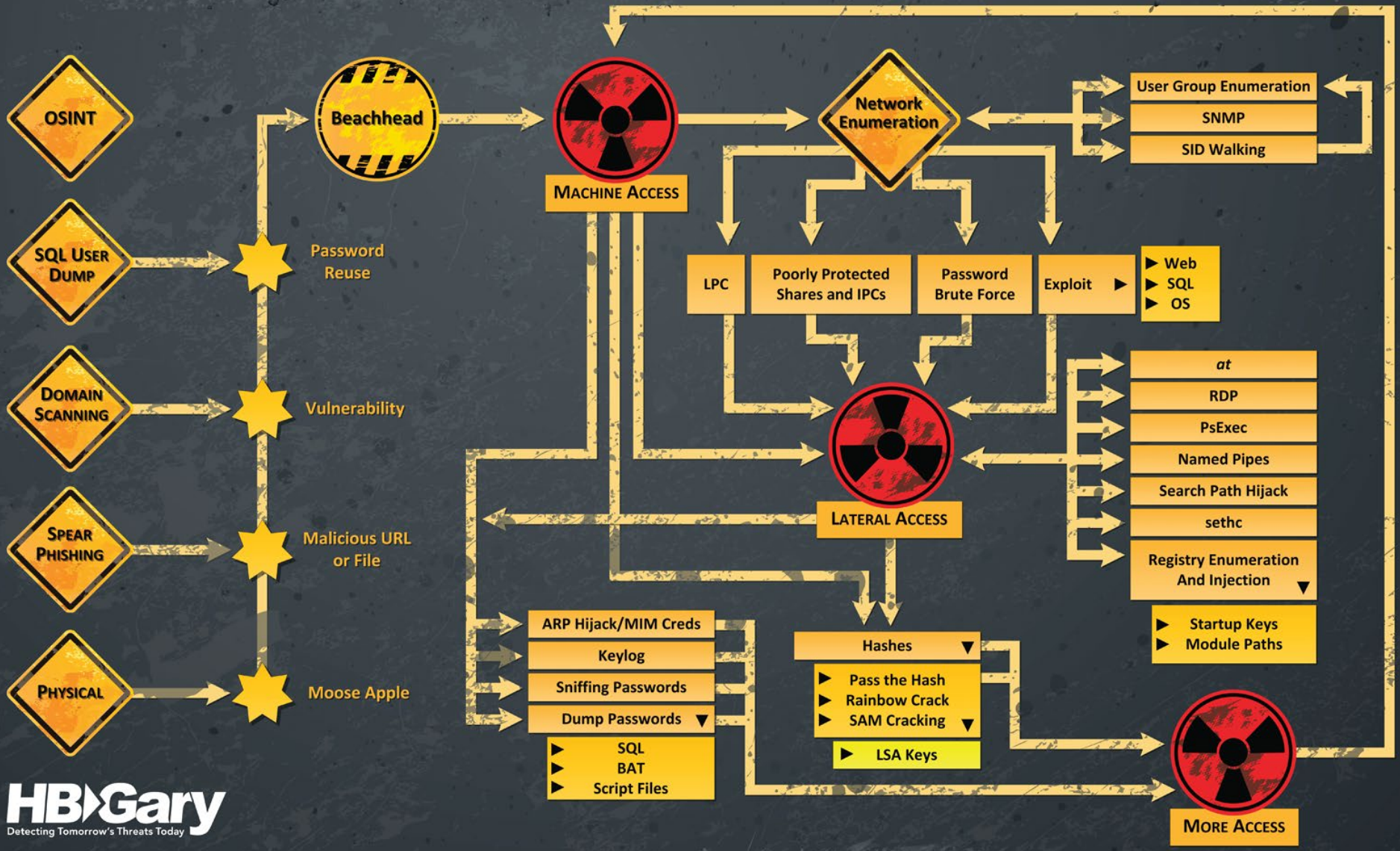
Security terms 3.

- **Forensics** – recover, analyze or gather data, evidence from computer systems to be used in court law
- **Black-box test** (vs. crystal-box) – testing with no knowledge of the test object's internal structure
- **Penetration test** - a method of evaluating the security of a computer system or network by simulating an attack from a malicious source
- **Security assessment** - an explicit study to locate IT security vulnerabilities and risk
- **Script kiddie** - a non-expert who breaks into computer systems by using pre-packaged automated tools written by other

Lateral movement

- SMB shares
- Password left in .bash_history (e.g. mysql –Ppassword)
- SSH .authorized_keys
- Root access -> “sudoers”?
- Pass the hash – mimikatz
- Sniffing network traffic (see: ARP spoofing, Ettercap) for passwords and information on infrastructure
- Simply finding new targets and hacking
- WPAD tricks (see Flame malware, Hot Potato Attack)
- Many other ways…

APT LATERAL MOVEMENT



HBGary
Detecting Tomorrow's Threats Today

Case Study: prezi hack

- See pdf

Certifications

- There are a number of certifications on products and on ethical hacking processes
- CISA,CISSP,OWASP,GIAC,OSCP,OSCE,etc.
- A certificate alone is useless
- However, it proves that some effort was put in to get the certificate (and money too)
- Both security personnel certifications, and product/system certifications can matter

Control questions

- What are the major steps of the hacking process?
- Why is it possible to hack into network systems?
- Identify some stakeholders related to the security of a system!
- Define black box testing!
- Why is it important to have independent security checks on your system?
- Why is it important to fix every single vulnerability?
- What is lateral movement?

Kiugró

- Miért feltörhetően a hálózati rendszerek?
- Mi az a script kiddie?
- Miért fontos a sérülékenységek kijavítása?
- Főnöke fel akarja törni az egyik szolgáltatót, ezért elkéri hozzá az ön jelszavát. Ön átadta. Szeretni elkerülni, hogy ezért megbüntessék, mit kell tennie?
- Mi a különbség egy állami hátterű célzott támadás és egy átlagos script kiddie támadása között