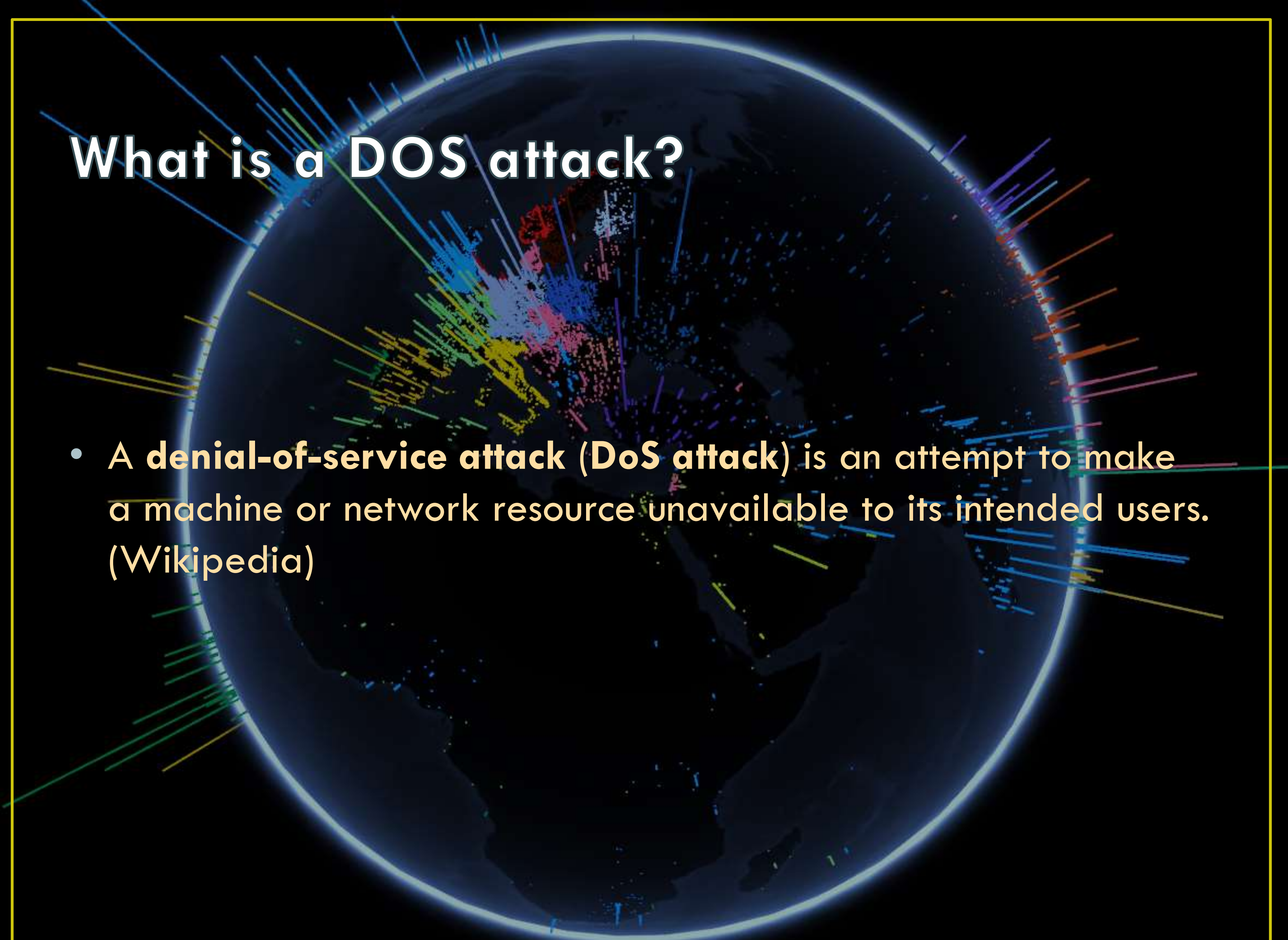
Denial of Service - Made Easy

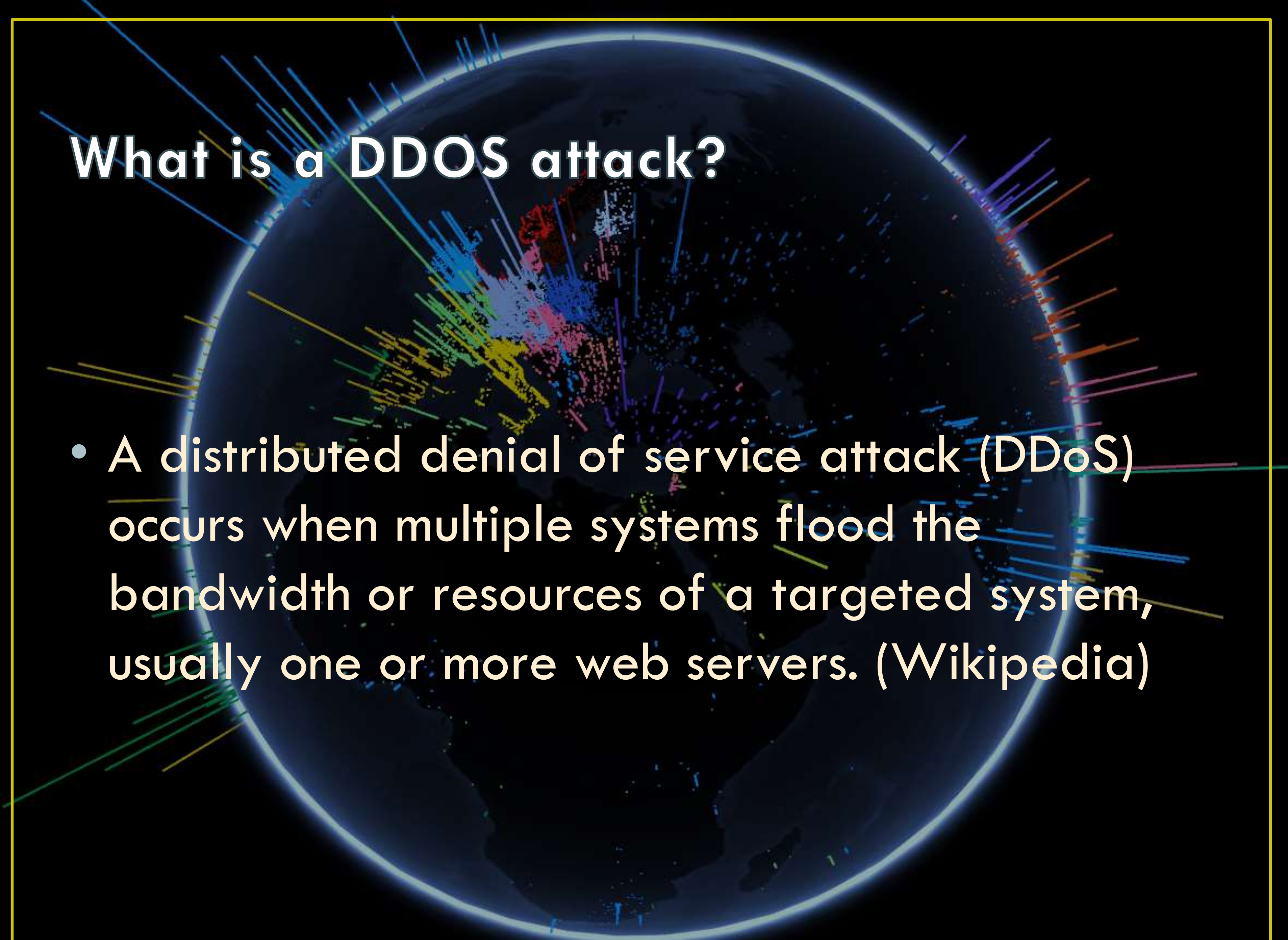
Yaniv Simsolo
CISSP

What is a DOS attack?



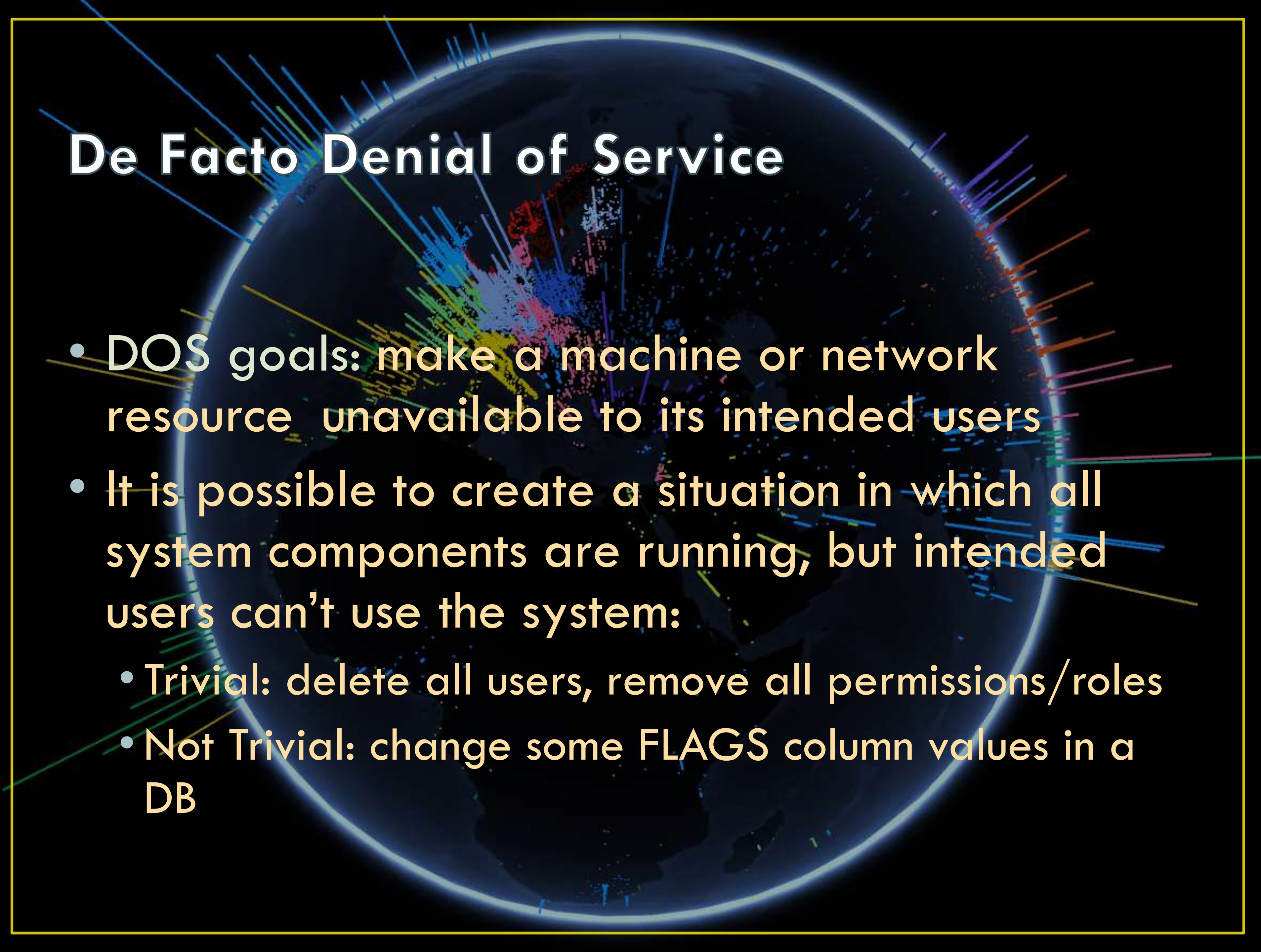
- A **denial-of-service attack** (**DoS attack**) is an attempt to make a machine or network resource unavailable to its intended users. (Wikipedia)

What is a DDOS attack?



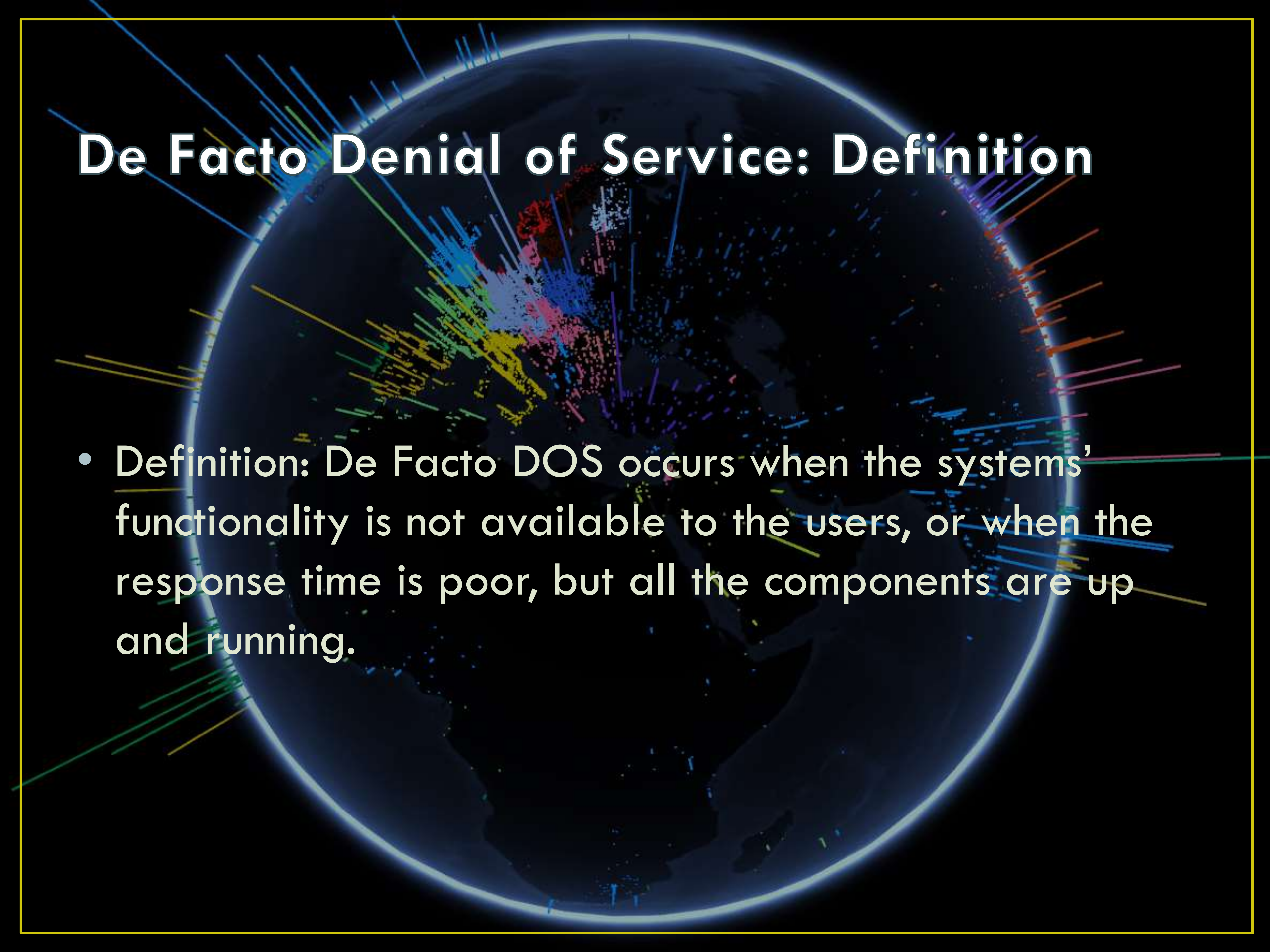
- A distributed denial of service attack (DDoS) occurs when multiple systems flood the bandwidth or resources of a targeted system, usually one or more web servers. (Wikipedia)

De Facto Denial of Service



- DOS goals: make a machine or network resource unavailable to its intended users
- It is possible to create a situation in which all system components are running, but intended users can’t use the system:
  - Trivial: delete all users, remove all permissions/roles
  - Not Trivial: change some FLAGS column values in a DB

De Facto Denial of Service: Definition



- Definition: De Facto DOS occurs when the systems' functionality is not available to the users, or when the response time is poor, but all the components are up and running.

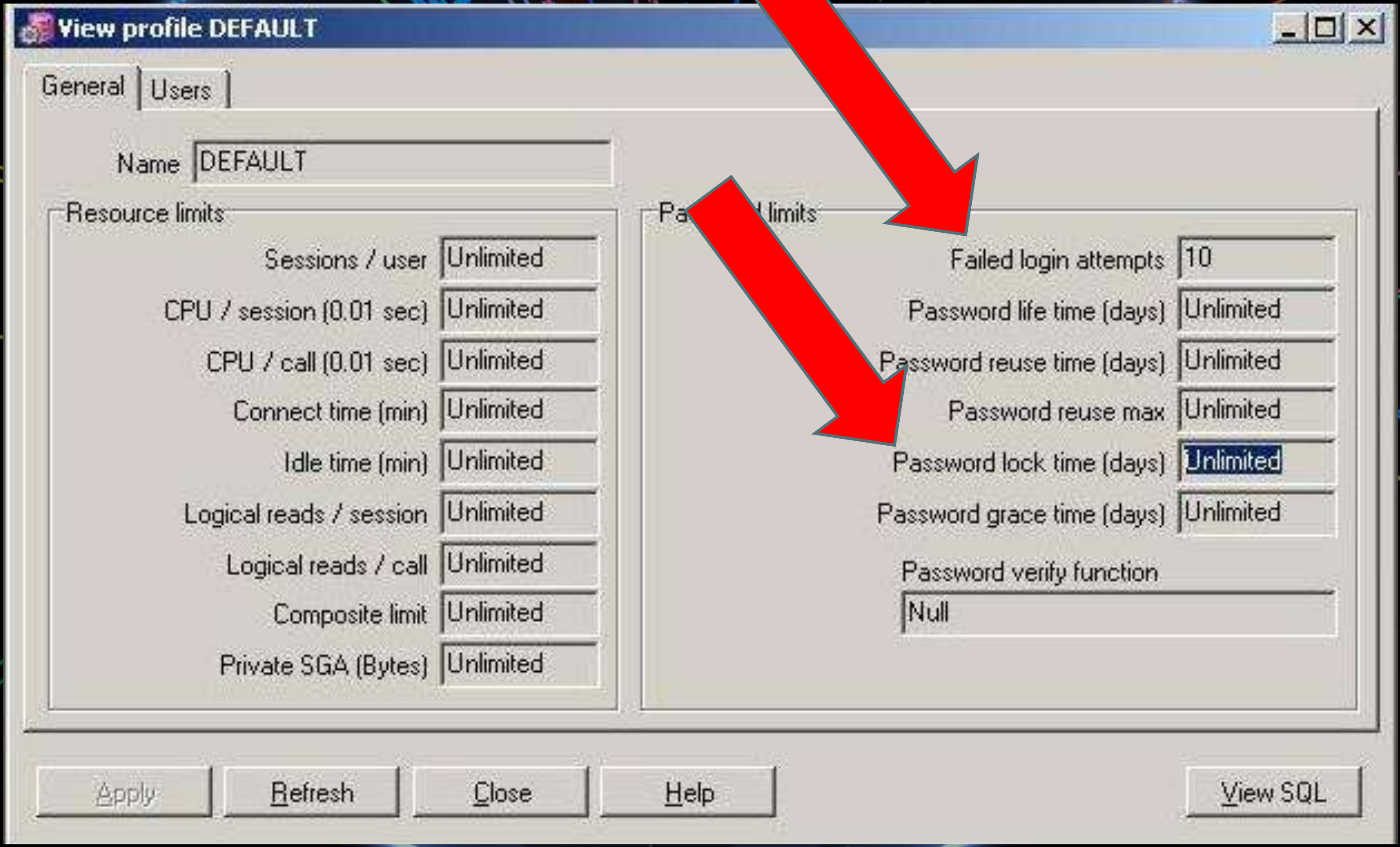
Obvious De Facto DOS

- A system allows for wildcard or nested queries
  - Common in “search” functionality
- Multiple calls for “heavy” actions (e.g. encryption)

Common Real-Life De Facto DOS – Oracle Databases

- By default, Oracle DBs supported systems are susceptible to De Facto DOS (versions 10, 11, Exadata)
  - All accounts are defined in a “User Profile”
  - By default, all the accounts (but few) are defined under the DEFAULT user profile
  - The DEFAULT user profile definition is “interesting”…

Oracle DEFAULT User Profile



View profile DEFAULT

Name: DEFAULT

Resource limits

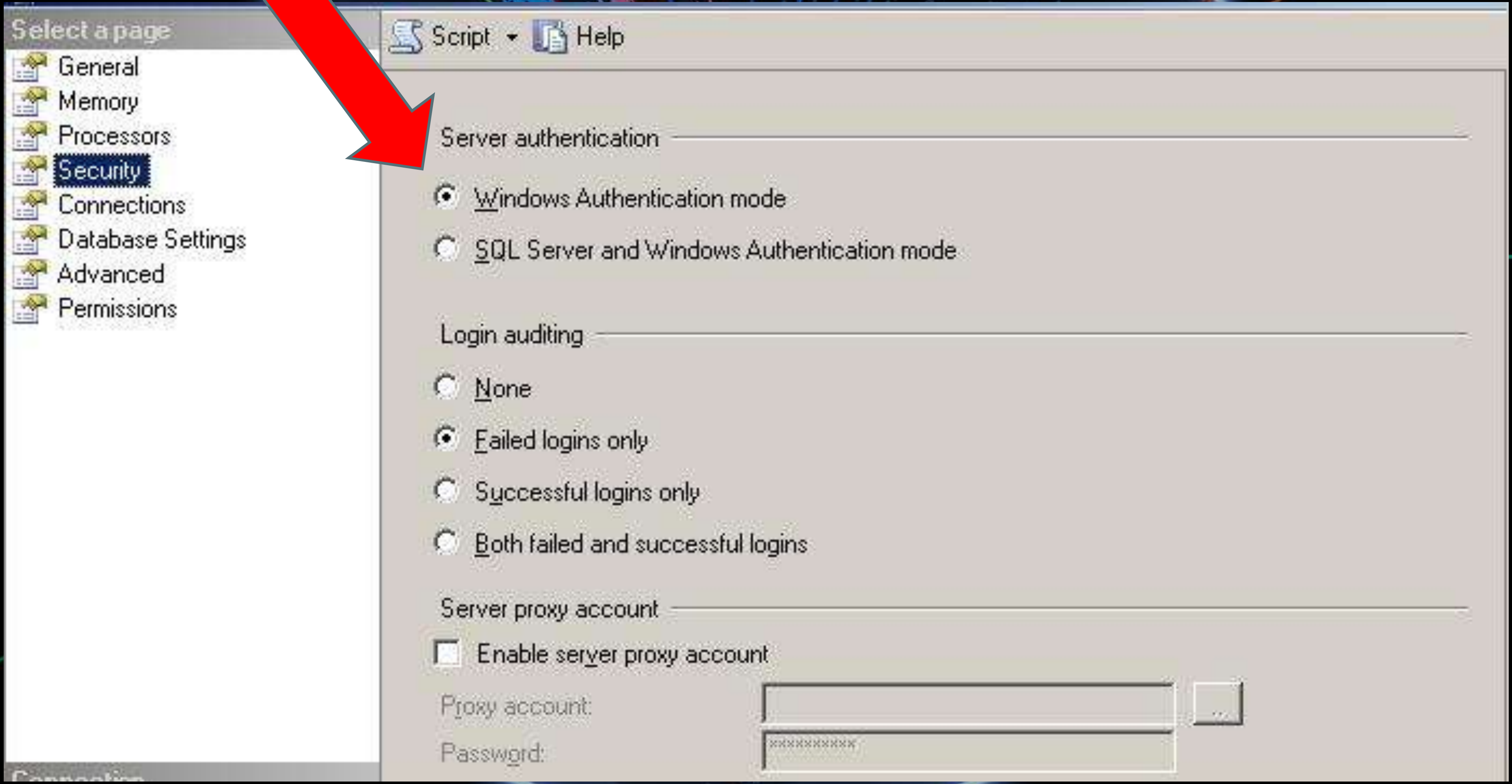
Sessions / user	Unlimited
CPU / session (0.01 sec)	Unlimited
CPU / call (0.01 sec)	Unlimited
Connect time (min)	Unlimited
Idle time (min)	Unlimited
Logical reads / session	Unlimited
Logical reads / call	Unlimited
Composite limit	Unlimited
Private SGA (Bytes)	Unlimited

Password limits

Failed login attempts	10
Password life time (days)	Unlimited
Password reuse time (days)	Unlimited
Password reuse max	Unlimited
Password lock time (days)	Unlimited
Password grace time (days)	Unlimited

Password verify function: Null

Common Real-Life De Facto DOS – SQL Server



Server authentication

● Windows Authentication mode

○ SQL Server and Windows Authentication mode

Login auditing

○ None

● Failed logins only

○ Successful logins only

○ Both failed and successful logins

Server proxy account

□ Enable server proxy account

Proxy account:

Password: ***********

Common Real-Life De Facto DOS – SQL Server

- SQL Server DBs may be susceptible to De Facto DOS, By Microsoft security recommendations…
  - Formal security documentations recommend: Windows Authentication to be configured in the SQL Server.
  - This is the recommendation for all accounts, including code entities.
  - Earlier versions of AD (prior to AD 2008) do not allow for a different lockout policy to different entities. All entities inherit the root lockout policy.
  - What is the root policy?

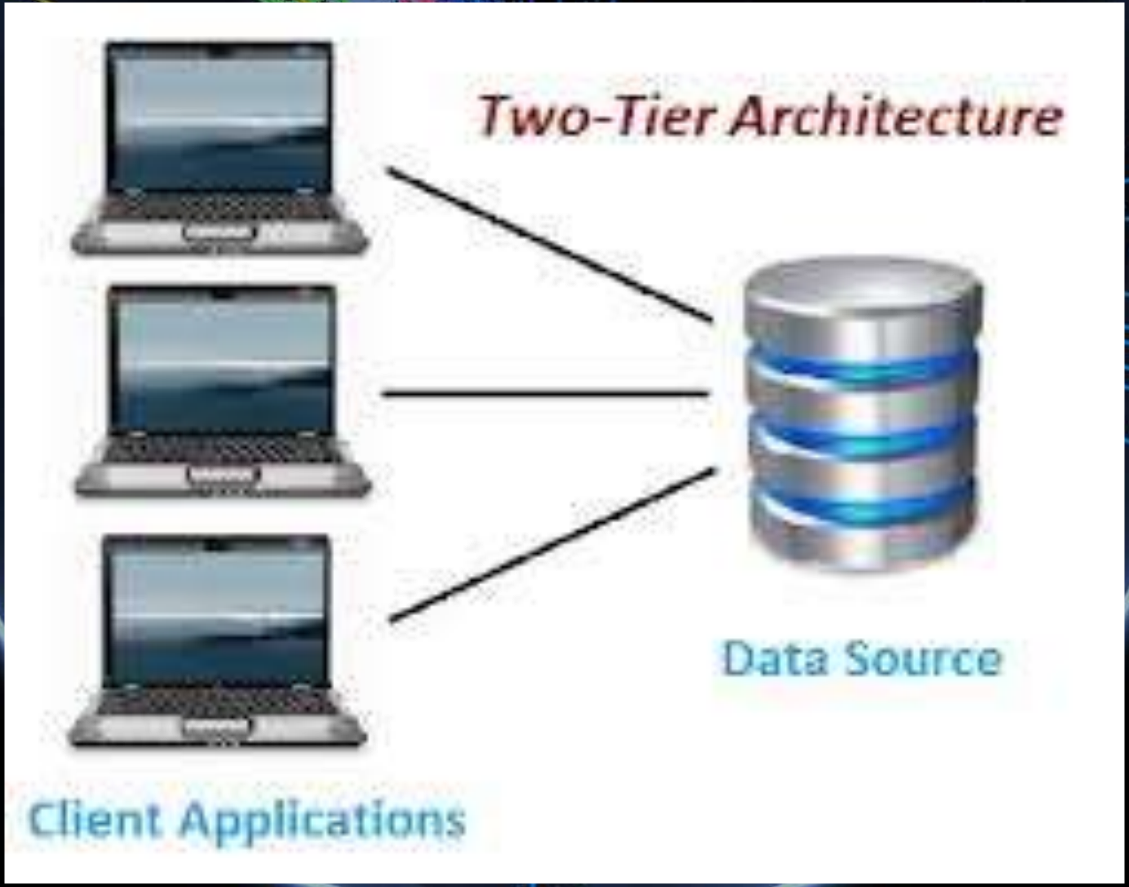
ADVANCED

Denial of Service

The Organization Hat

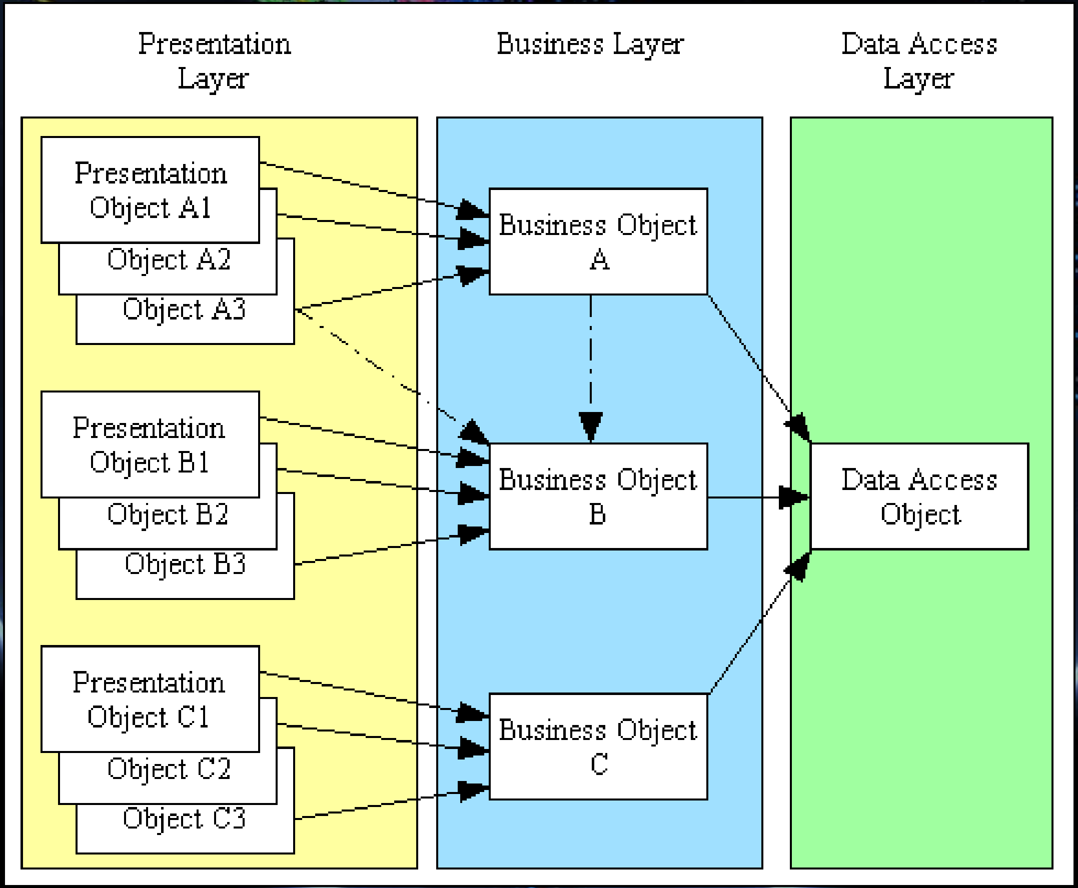
Once Upon a Time

- Two-Tier Architecture



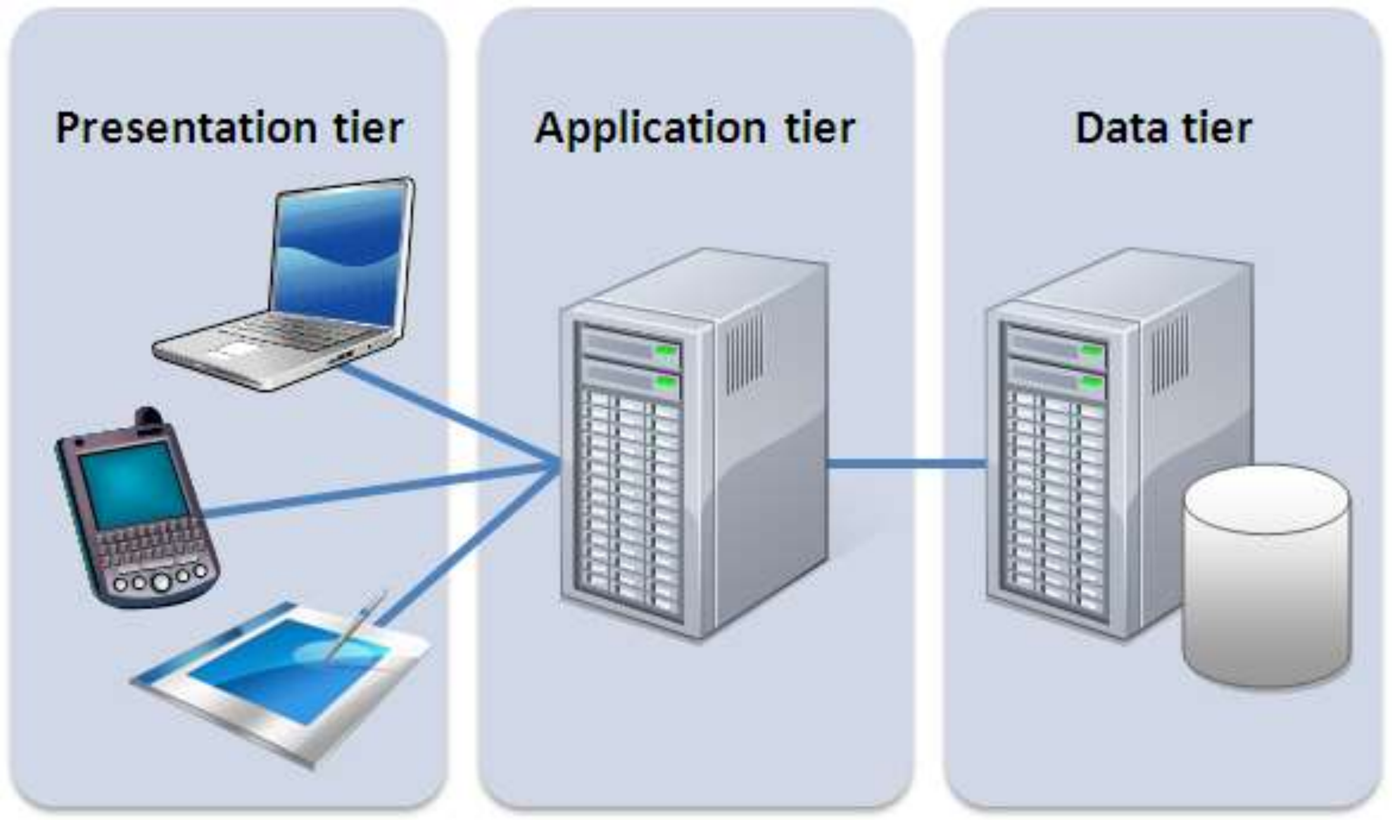
Once Upon a Time

- The roots of Three-Tier Architecture



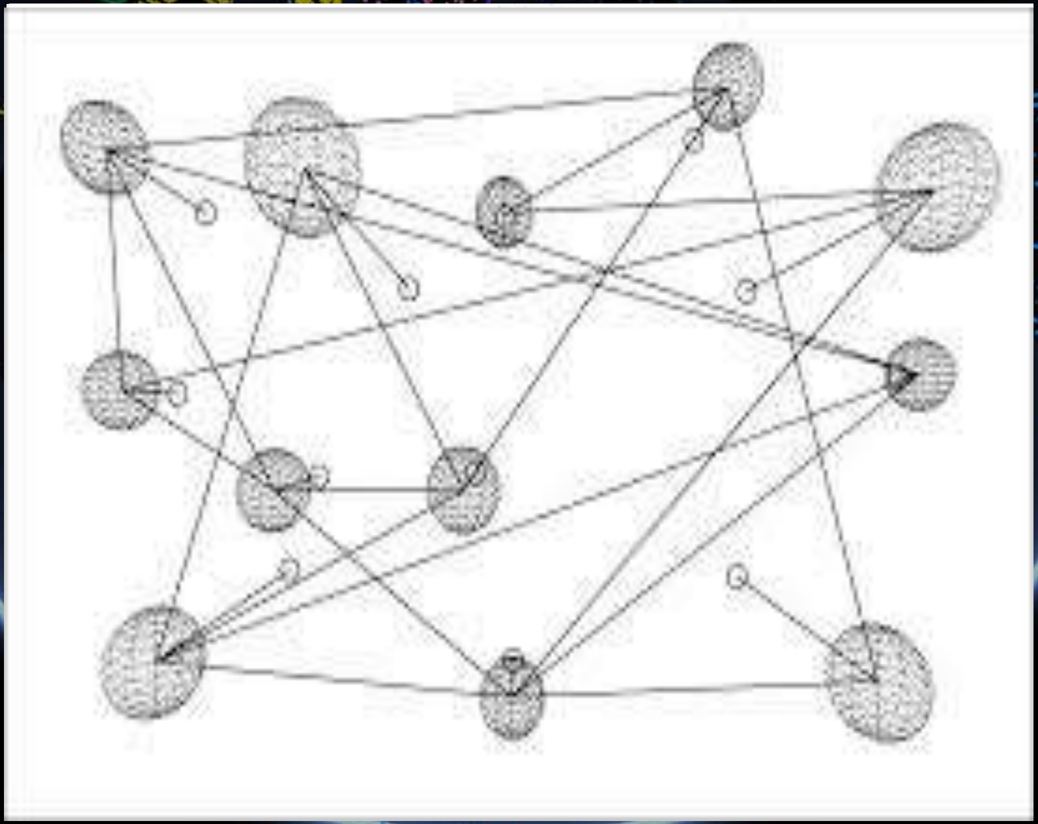
Almost there…

- Concurrent Three-Tier Architecture, the presentation tier migrated elsewhere.



Modern Systems Architecture

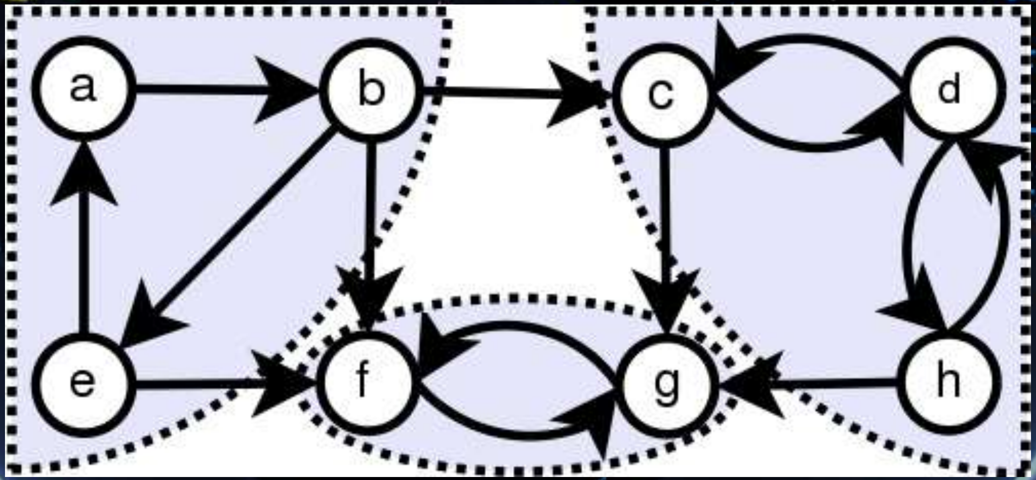
- Not a simple graph any more…



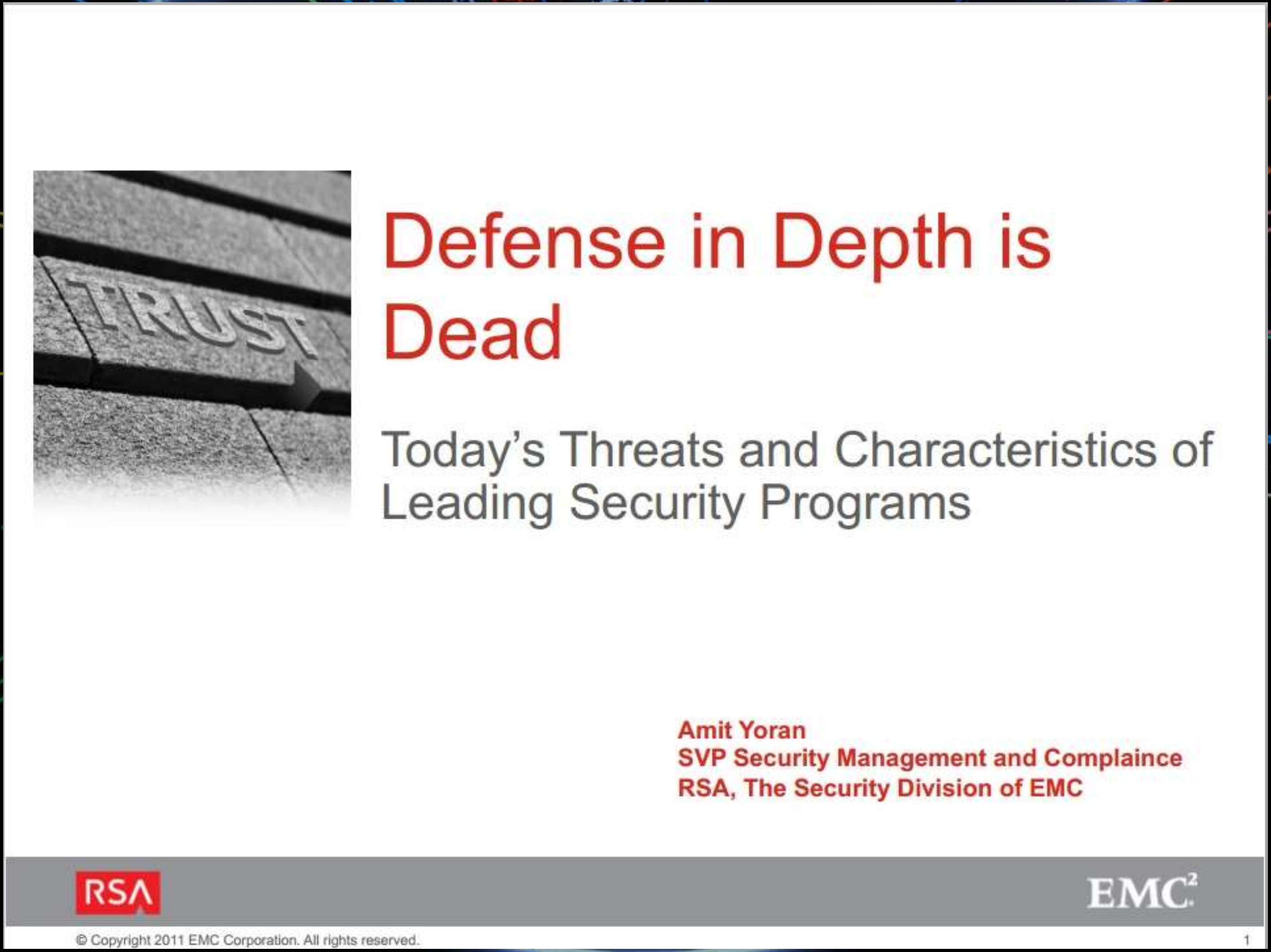
Modern Systems Architecture

- Not a simple graph any more…

(Strongly connected graph)



Overly Complex Systems



Defense in Depth is Dead

Today's Threats and Characteristics of Leading Security Programs

Amit Yoran
SVP Security Management and Complaince
RSA, The Security Division of EMC

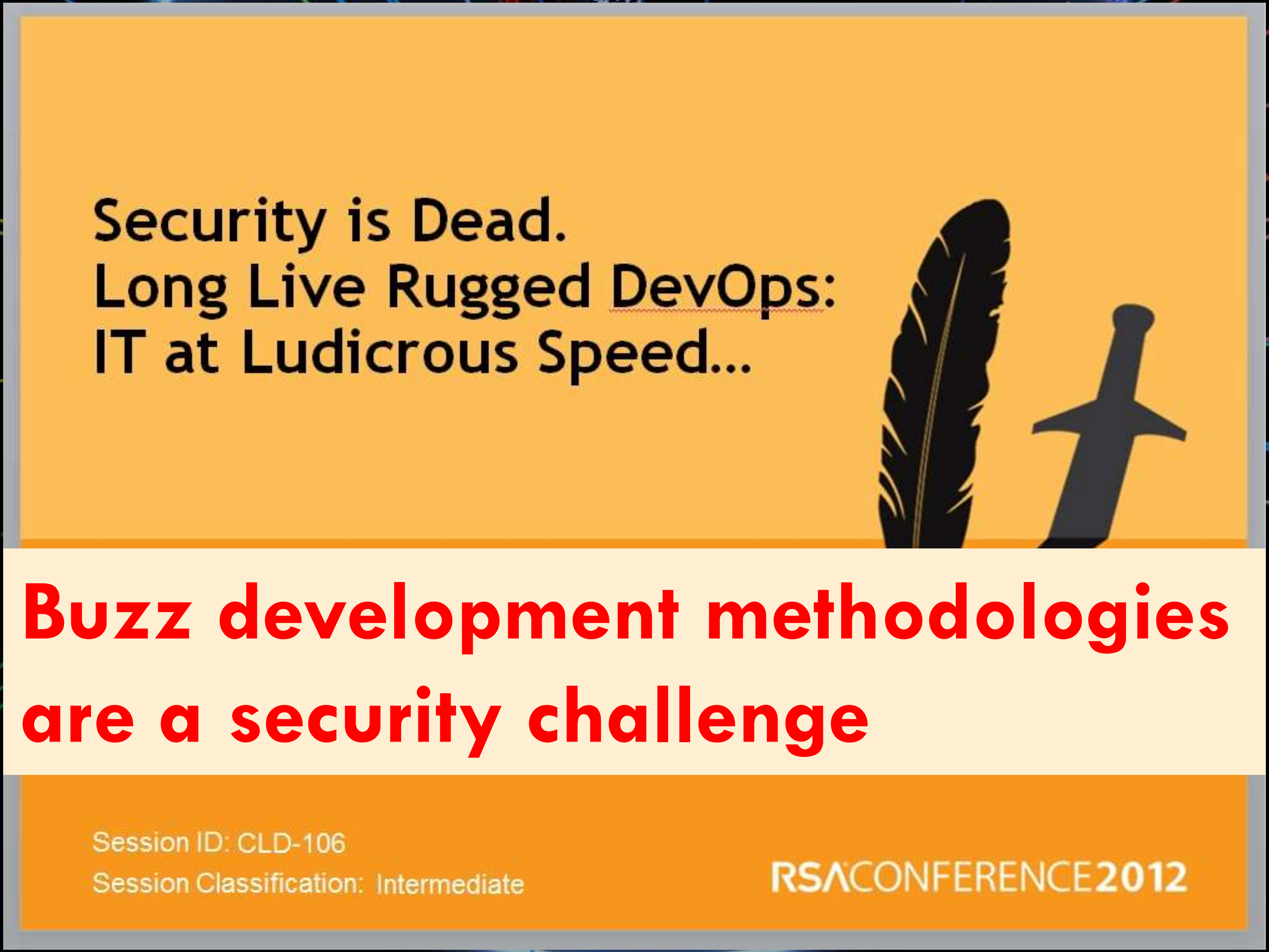
Overly Complex Systems

- Defense In-Depth is dead.

Overly Complex Systems

- Defense In-Depth is dead.
- Is this better?

Overly Complex Systems



Security is Dead.
Long Live Rugged DevOps:
IT at Ludicrous Speed...

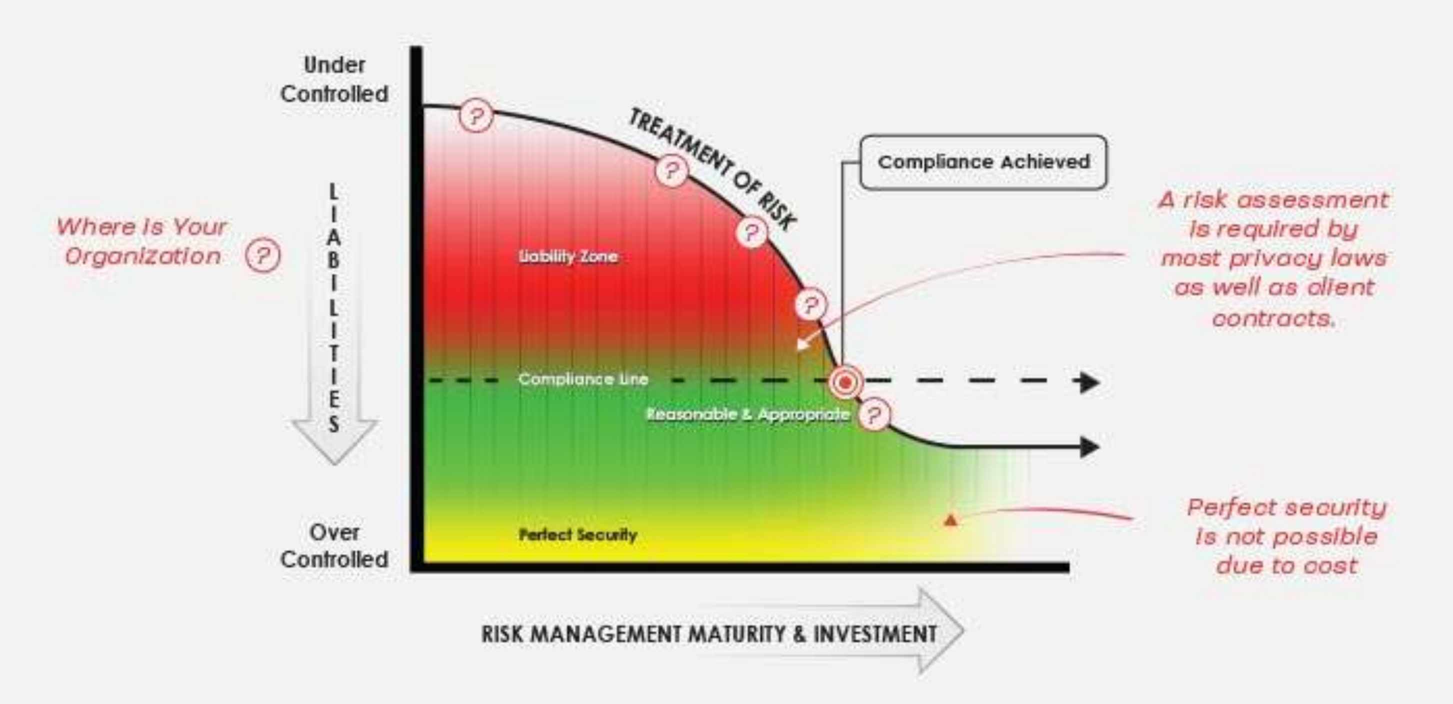
Session ID: CLD-106
Session Classification: Intermediate

RSACONFERENCE2012

Buzz development methodologies are a security challenge

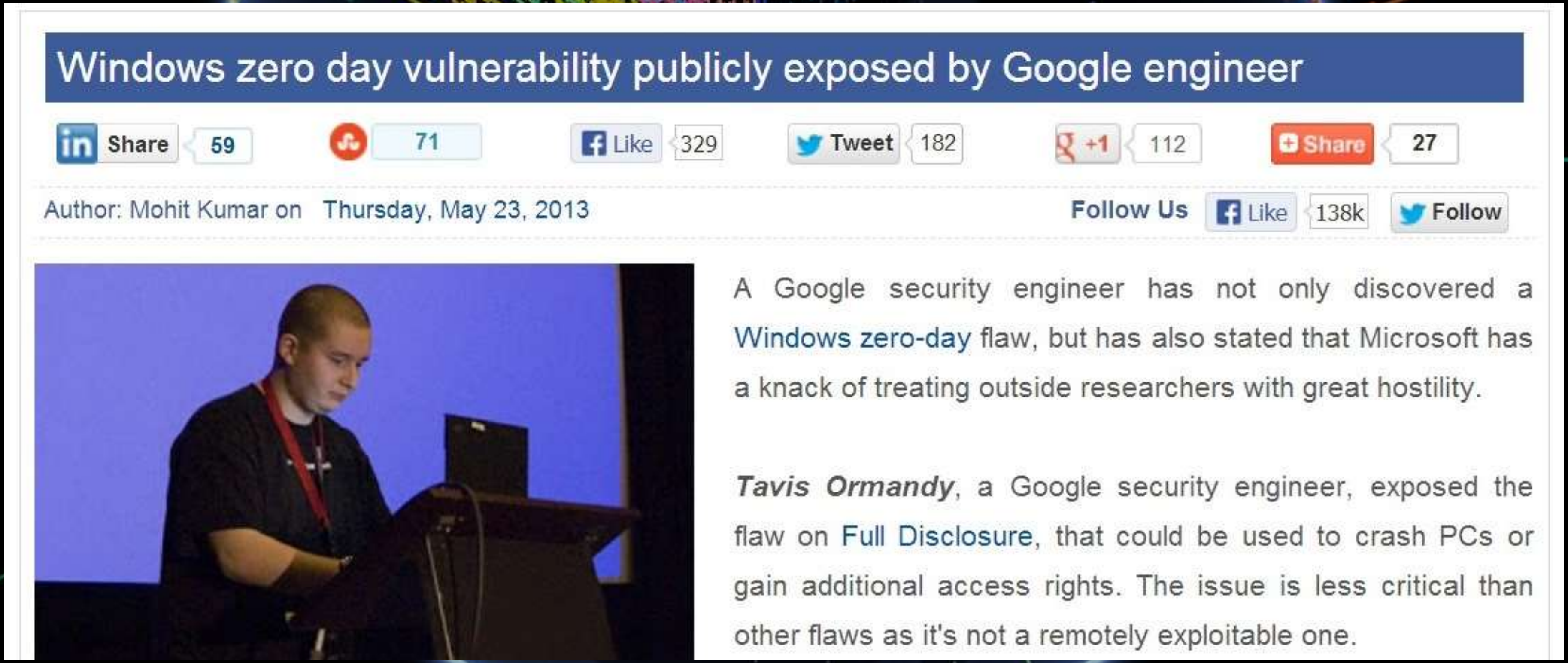
Overly Complex Systems

- Reality check: it is VERY difficult to maintain high security level


Under Controlled
L I A B I L I T I E S
Over Controlled
Where Is Your Organization ?
TREATMENT OF RISK
Compliance Achieved
Liability Zone
Compliance Line
Reasonable & Appropriate
Perfect Security
A risk assessment is required by most privacy laws as well as client contracts.
Perfect security is not possible due to cost
RISK MANAGEMENT MATURITY & INVESTMENT

S-SDLC is Dead

- Reality check:



Windows zero day vulnerability publicly exposed by Google engineer

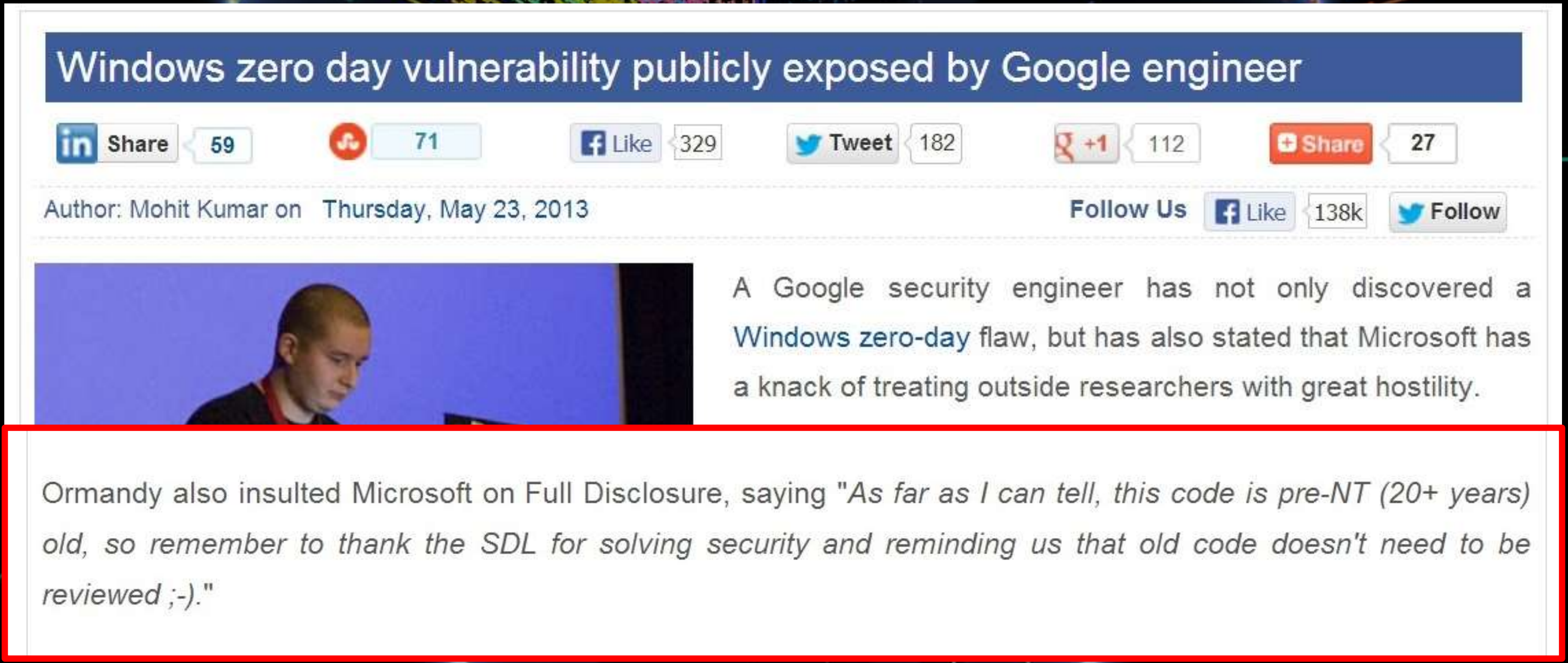
Author: Mohit Kumar on Thursday, May 23, 2013

A Google security engineer has not only discovered a Windows zero-day flaw, but has also stated that Microsoft has a knack of treating outside researchers with great hostility.

Tavis Ormandy, a Google security engineer, exposed the flaw on Full Disclosure, that could be used to crash PCs or gain additional access rights. The issue is less critical than other flaws as it's not a remotely exploitable one.

S-SDLC is Dead

- Reality check:



Windows zero day vulnerability publicly exposed by Google engineer

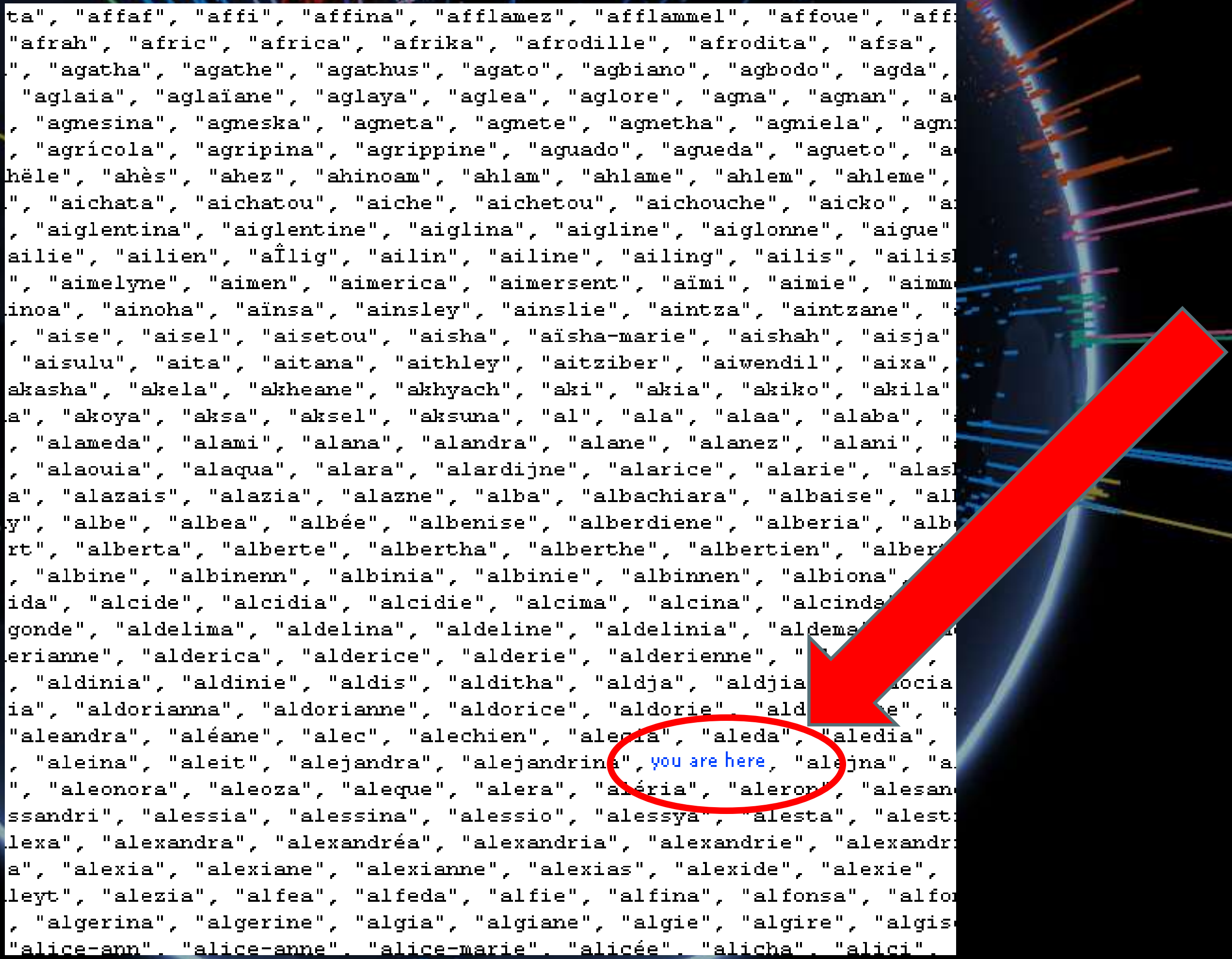
Author: Mohit Kumar on Thursday, May 23, 2013

A Google security engineer has not only discovered a Windows zero-day flaw, but has also stated that Microsoft has a knack of treating outside researchers with great hostility.

Ormandy also insulted Microsoft on Full Disclosure, saying "*As far as I can tell, this code is pre-NT (20+ years) old, so remember to thank the SDL for solving security and reminding us that old code doesn't need to be reviewed ;-).*"

The Hacker Hat

Our Mission? Locate the DOS!



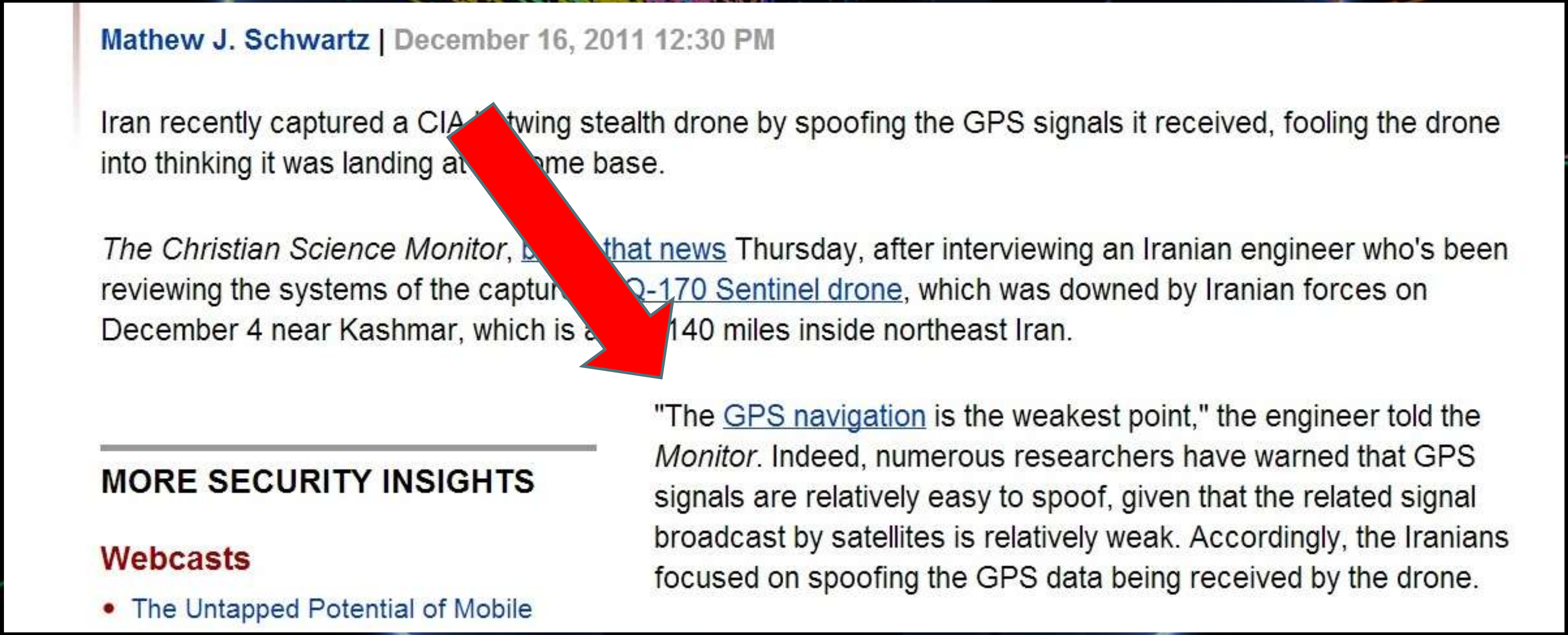
```
ta", "affaf", "affi", "affina", "afflamez", "afflammel", "affoue", "aff
"afrah", "afric", "africa", "afrika", "afrodille", "afrodita", "afsa",
", "agatha", "agathe", "agathus", "agato", "agbiano", "agbodo", "agda",
 "aglaia", "aglaïane", "aglaya", "aglea", "aglore", "agna", "agnan", "a
, "agnesina", "agneska", "agneta", "agnete", "agnetha", "agniela", "agn
, "agricola", "agripina", "agrippine", "aguado", "agueda", "agueto", "a
hële", "ahès", "ahez", "ahinoam", "ahlam", "ahlame", "ahlem", "ahleme",
", "aichata", "aichatou", "aiche", "aichetou", "aichouche", "aicko", "a
, "aiglentina", "aiglentine", "aiglina", "aigline", "aiglonne", "aigue"
ailie", "ailien", "aÎlig", "ailin", "ailine", "ailing", "ailis", "ailis
", "aimelyne", "aimen", "aimerica", "aimersent", "aïmi", "aimie", "aimm
inoa", "ainoha", "aïnsa", "ainsley", "ainslie", "aintza", "aintzane", "
, "aise", "aisel", "aisetou", "aisha", "aïsha-marie", "aishah", "aisja"
 "aisulu", "aita", "aitana", "aithley", "aitziber", "aiwendil", "aixa",
akasha", "akela", "akheane", "akhyach", "aki", "akia", "akiko", "akila"
a", "akoya", "aksa", "aksel", "aksuna", "al", "ala", "alaa", "alaba", "
, "alameda", "alami", "alana", "alandra", "alane", "alanez", "alani", "
, "alaouia", "alaqua", "alara", "alardijne", "alarice", "alarie", "alas
a", "alazais", "alazia", "alazne", "alba", "albachiara", "albaise", "al
y", "albe", "albea", "albée", "albenise", "alberdiene", "alberia", "alb
rt", "alberta", "alberte", "albertha", "alberthe", "albertien", "alber
, "albine", "albinenn", "albinia", "albinie", "albinnen", "albiona",
ida", "alcide", "alcidia", "alcidie", "alcima", "alcina", "alcinda
gonde", "aldelima", "aldelina", "aldeline", "aldelinia", "aldema
erianne", "alderica", "alderice", "alderie", "alderienne", "
, "aldinia", "aldinie", "aldis", "alditha", "aldja", "aldjia ocia
ia", "aldorianna", "aldorianne", "aldorice", "aldorie", "ald e", "
"aleandra", "aléane", "alec", "alechien", "alecia", "aleda", "aledia",
, "aleina", "aleit", "alejandra", "alejandrina", you are here, "alejna", "a
", "aleonora", "aleoza", "aleque", "alera", "aléria", "aleron", "alesan
ssandri", "alessia", "alessina", "alessio", "alessya", "alesta", "alest
lexa", "alexandra", "alexandréa", "alexandria", "alexandrie", "alexandr
a", "alexia", "alexiane", "alexianne", "alexias", "alexide", "alexie",
leyt", "alezia", "alfea", "alfeda", "alfie", "alfina", "alfonsa", "alfo
, "algerina", "algerine", "algia", "algiane", "algie", "algire", "algis
"alice-ann", "alice-anne", "alice-marie", "alicée", "alicha", "alici",
```

Our Mission?

The *Mission*: Any Shortcuts?

Yep! Shortcuts Time

- In 2012 a US drone airplane forced to land in Iran



Mathew J. Schwartz | December 16, 2011 12:30 PM

Iran recently captured a CIA [illegible]twing stealth drone by spoofing the GPS signals it received, fooling the drone into thinking it was landing at [illegible]me base.

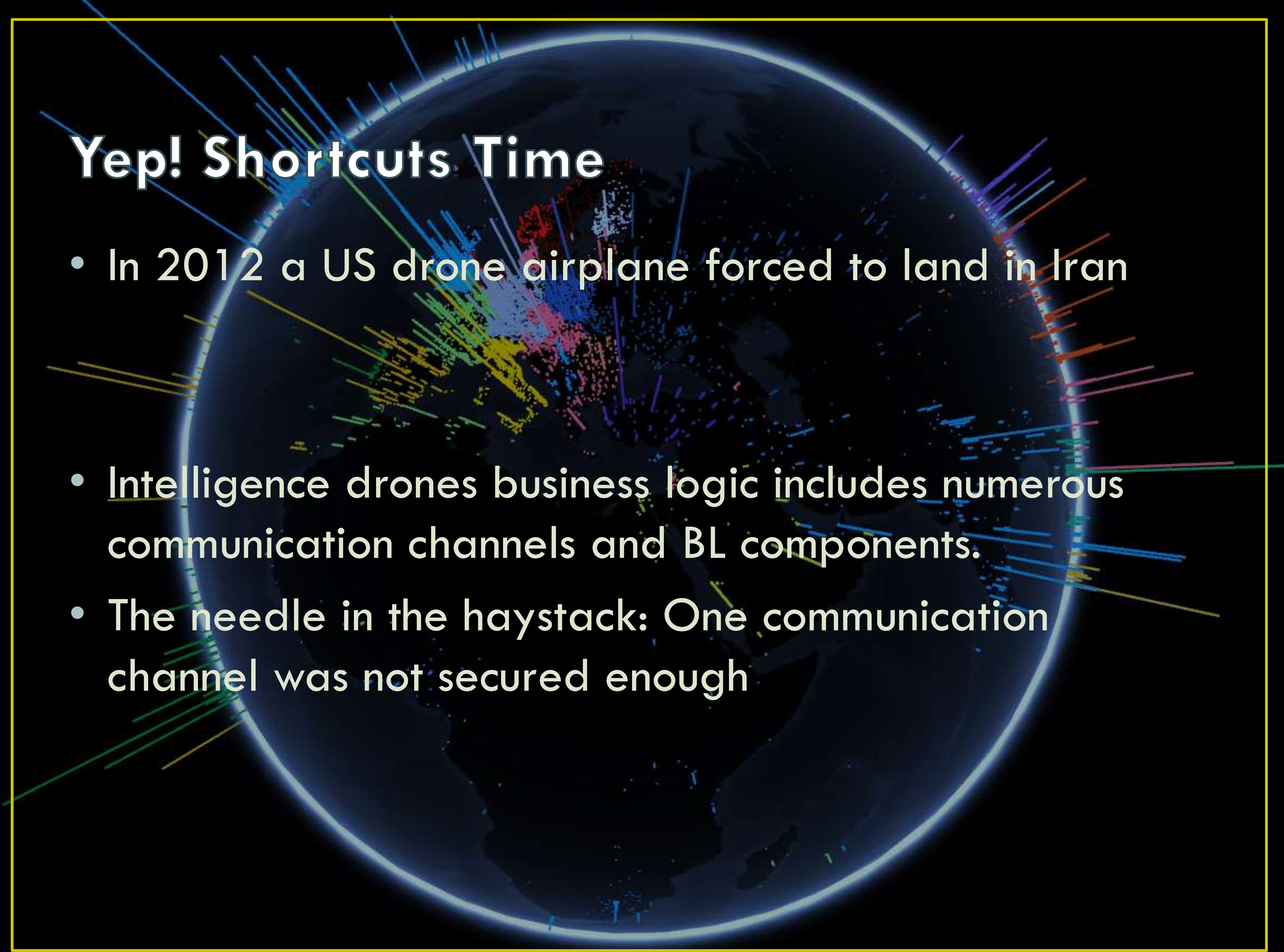
The Christian Science Monitor, b[illegible] that news Thursday, after interviewing an Iranian engineer who's been reviewing the systems of the captur[illegible]Q-170 Sentinel drone, which was downed by Iranian forces on December 4 near Kashmar, which is a[illegible] 140 miles inside northeast Iran.

"The GPS navigation is the weakest point," the engineer told the *Monitor*. Indeed, numerous researchers have warned that GPS signals are relatively easy to spoof, given that the related signal broadcast by satellites is relatively weak. Accordingly, the Iranians focused on spoofing the GPS data being received by the drone.

MORE SECURITY INSIGHTS

Webcasts

- The Untapped Potential of Mobile

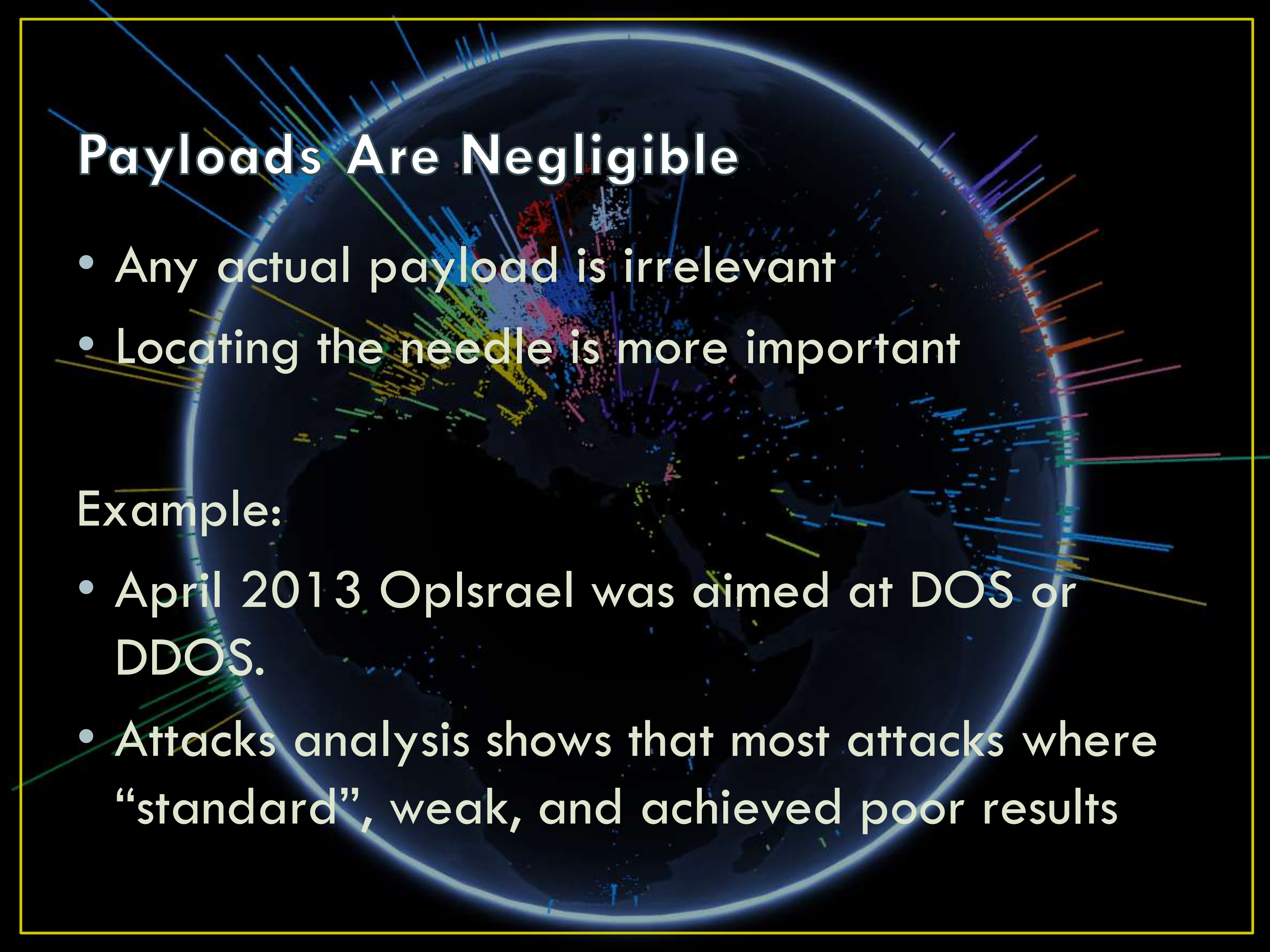


Yep! Shortcuts Time

- In 2012 a US drone airplane forced to land in Iran

- Intelligence drones business logic includes numerous communication channels and BL components.
- The needle in the haystack: One communication channel was not secured enough

Slaying a Sacred Cow, Take 1



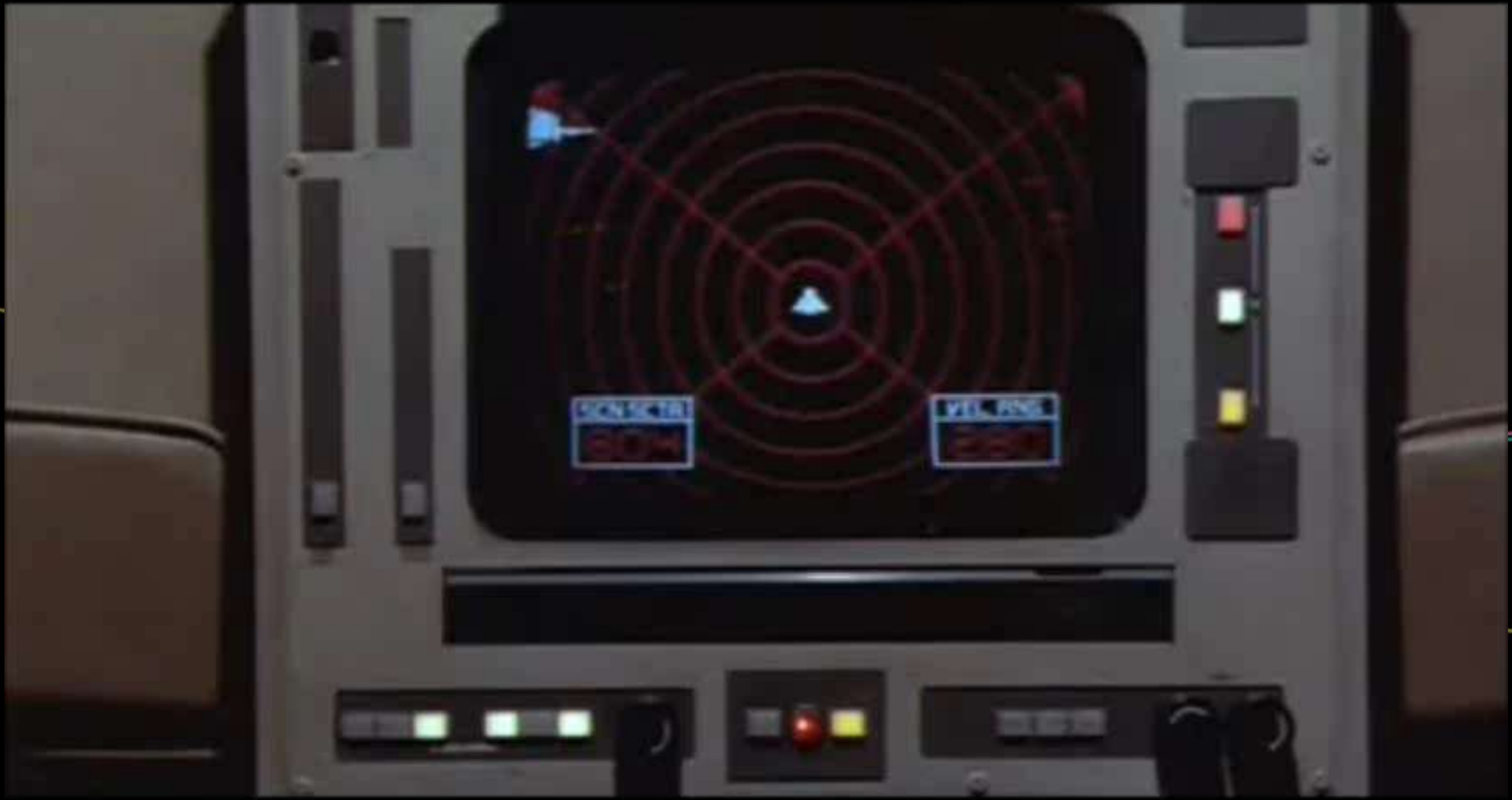
Payloads Are Negligible

- Any actual payload is irrelevant
- Locating the needle is more important

Example:

- April 2013 OpIsrael was aimed at DOS or DDOS.
- Attacks analysis shows that most attacks where “standard”, weak, and achieved poor results

Sci-Fi Attack Vectors?

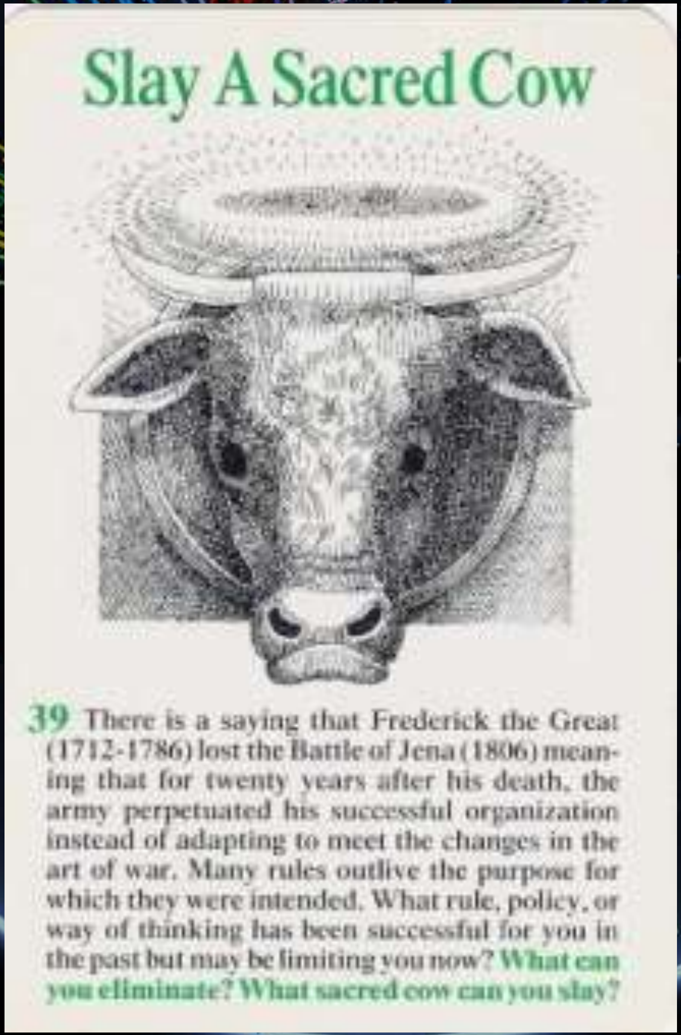

SCN SCTR
VEL ANG

Ludicrous Attack Vectors

Ludicrous Attack Vectors – Lockheed Martin Hack

- Determination - a key in locating the needle.
- Ludicrous attacks are in the hood: Watering hole and SpearPhishing were employed.
- The attack: "fairly subtle", yet "significant and tenacious"

Slaying a Sacred Cow, Take 2



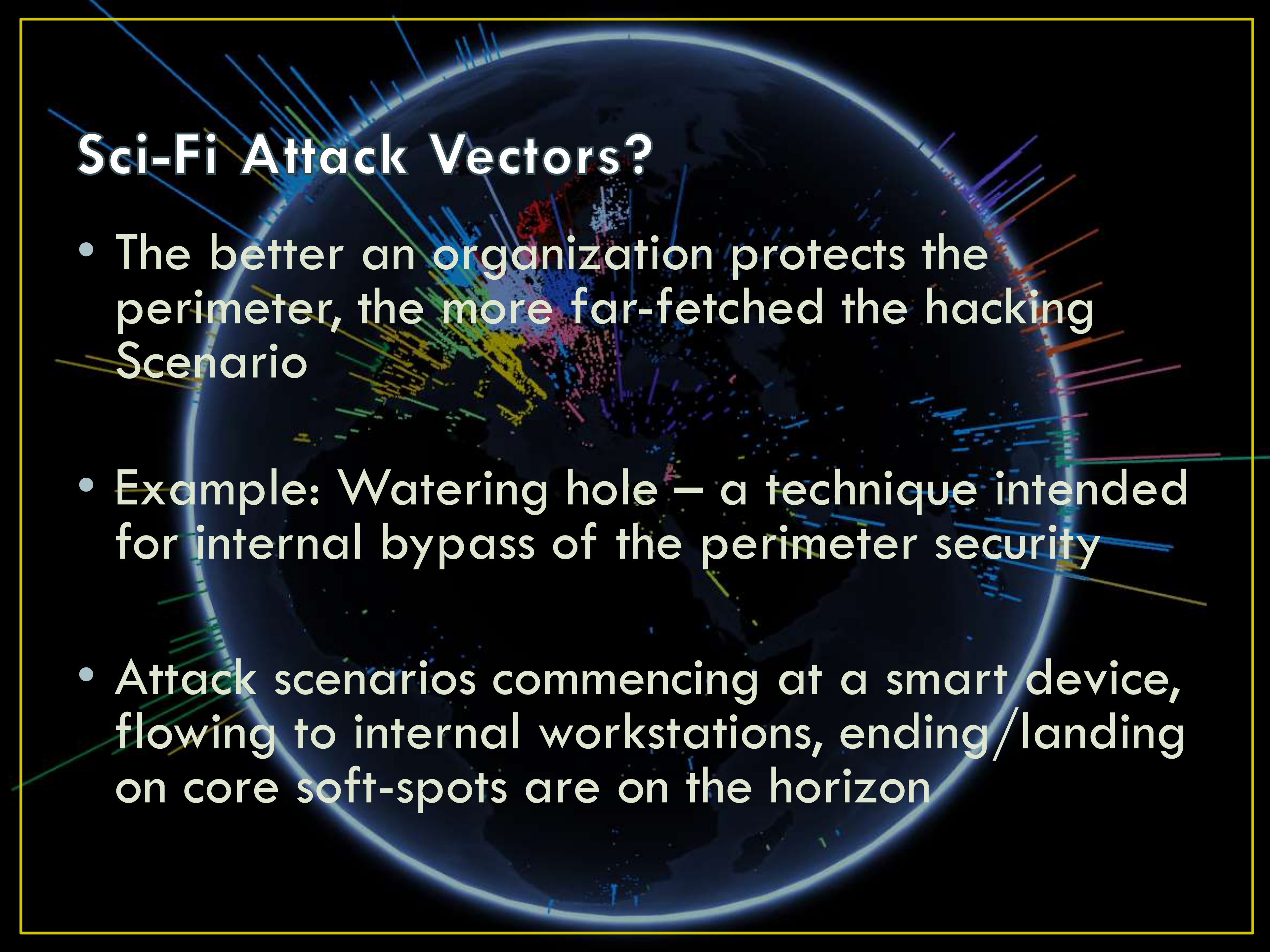
Slay A Sacred Cow

39 There is a saying that Frederick the Great (1712-1786) lost the Battle of Jena (1806) meaning that for twenty years after his death, the army perpetuated his successful organization instead of adapting to meet the changes in the art of war. Many rules outlive the purpose for which they were intended. What rule, policy, or way of thinking has been successful for you in the past but may be limiting you now? **What can you eliminate? What sacred cow can you slay?**

Two Factor Authentication is Dead ?
Lockheed Martin Hack

- Mr. Ed Schwartz, VP and CISO, RSA, the Security Division of EMC: "**Recently we learned that two factor authentication is not enough anymore**",
  - Managing Advanced Security Threats Using Big Data Analytics, International Cyber Conference II,

    Israel, June 2012



Sci-Fi Attack Vectors?

- The better an organization protects the perimeter, the more far-fetched the hacking Scenario

- Example: Watering hole – a technique intended for internal bypass of the perimeter security

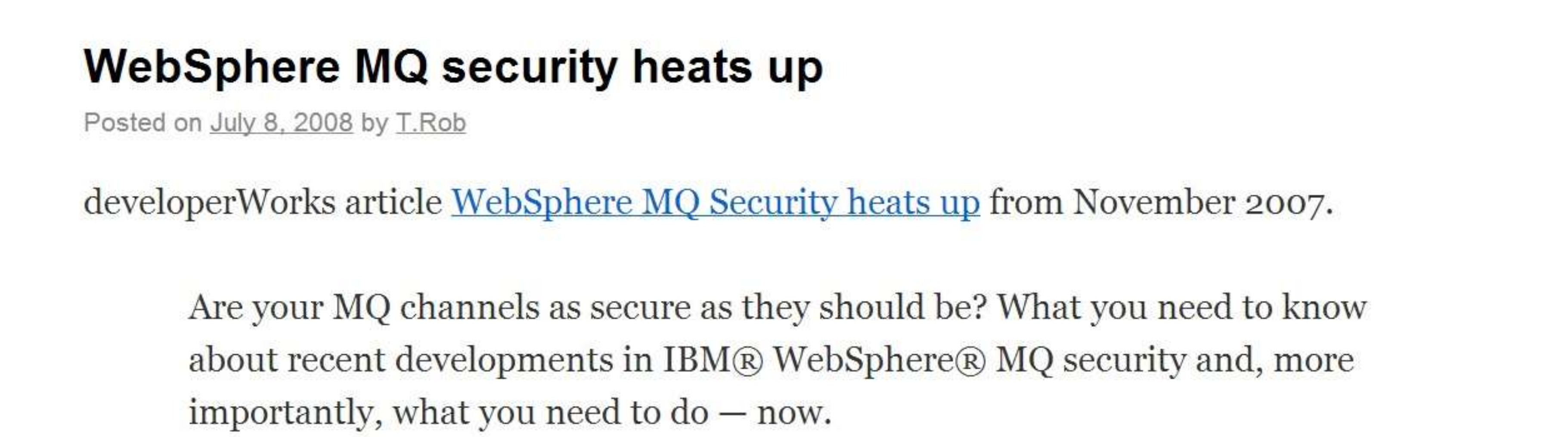
- Attack scenarios commencing at a smart device, flowing to internal workstations, ending/landing on core soft-spots are on the horizon

Sci-Fi Attack Vectors?

- SSL is dead
- FW is dead
- IPS/IDS is dead
- Anti Virus is dead
- [insert security product X here] is dead:
  - XML FW, DB FW,

Where Is The Shortcut?

Real-Life De Facto DOS – MQ Infrastructure



WebSphere MQ security heats up

Posted on July 8, 2008 by T.Rob

developerWorks article WebSphere MQ Security heats up from November 2007.

> Are your MQ channels as secure as they should be? What you need to know about recent developments in IBM® WebSphere® MQ security and, more importantly, what you need to do — now.

WebSphere MQ had been in the market 14 years when this article was published. During that time the two big changes to the product's security posture were to set MCAUSER blank by default due to strong customer feedback, and the addition of SSL as a channel option. The first made WMQ wide open by default and the second was only used by a relatively few customers. Over the years, WMQ security was systematically ignored by users and hackers alike.

Real-Life De Facto DOS – MQ Infrastructure

- How far can a VERY easy DOS De Facto attack affect an organization?
- **Do organizations audit MQ security?**

Even Worse… DOS By Design

- Even when everything is OK, changes to programming key features brings DOS even closer
- Siebel & IE6 Example

Even Worse... DOS By Design

- Sci Fi or Far-Fetched Scenario?
  - US department of homeland security calls on computer users to disable java

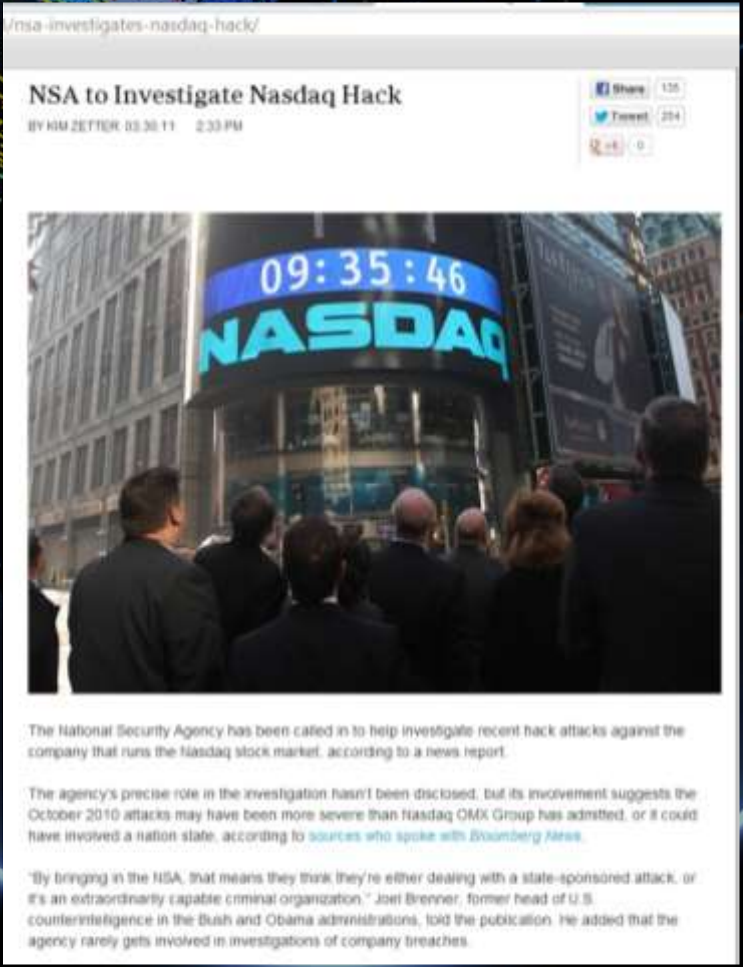
???

- Java 6.19 & Java 7.21 mixed code policy

Where Is The Shortcut?

Ultimate DOS

- NASDAQ, 2011, Commerce stopped due to internal DOS attack



/nsa-investigates-nasdaq-hack/

NSA to Investigate Nasdaq Hack

BY KIM ZETTER 03.30.11 2:33 PM

The National Security Agency has been called in to help investigate recent hack attacks against the company that runs the Nasdaq stock market, according to a news report.

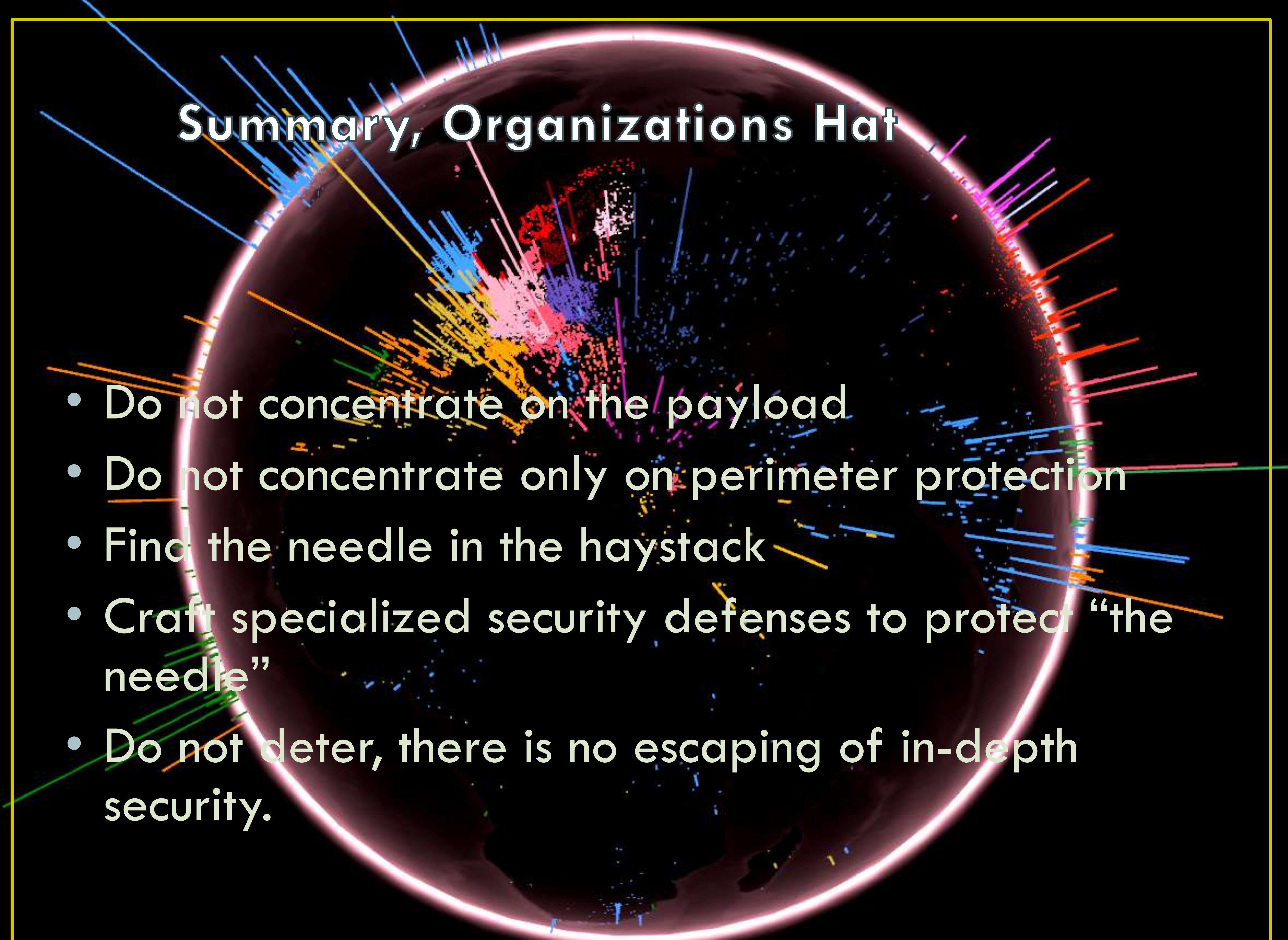
The agency's precise role in the investigation hasn't been disclosed, but its involvement suggests the October 2010 attacks may have been more severe than Nasdaq OMX Group has admitted, or it could have involved a nation state, according to sources who spoke with Bloomberg News.

"By bringing in the NSA, that means they think they're either dealing with a state-sponsored attack, or it's an extraordinarily capable criminal organization," Joel Brenner, former head of U.S. counterintelligence in the Bush and Obama administrations, told the publication. He added that the agency rarely gets involved in investigations of company breaches.

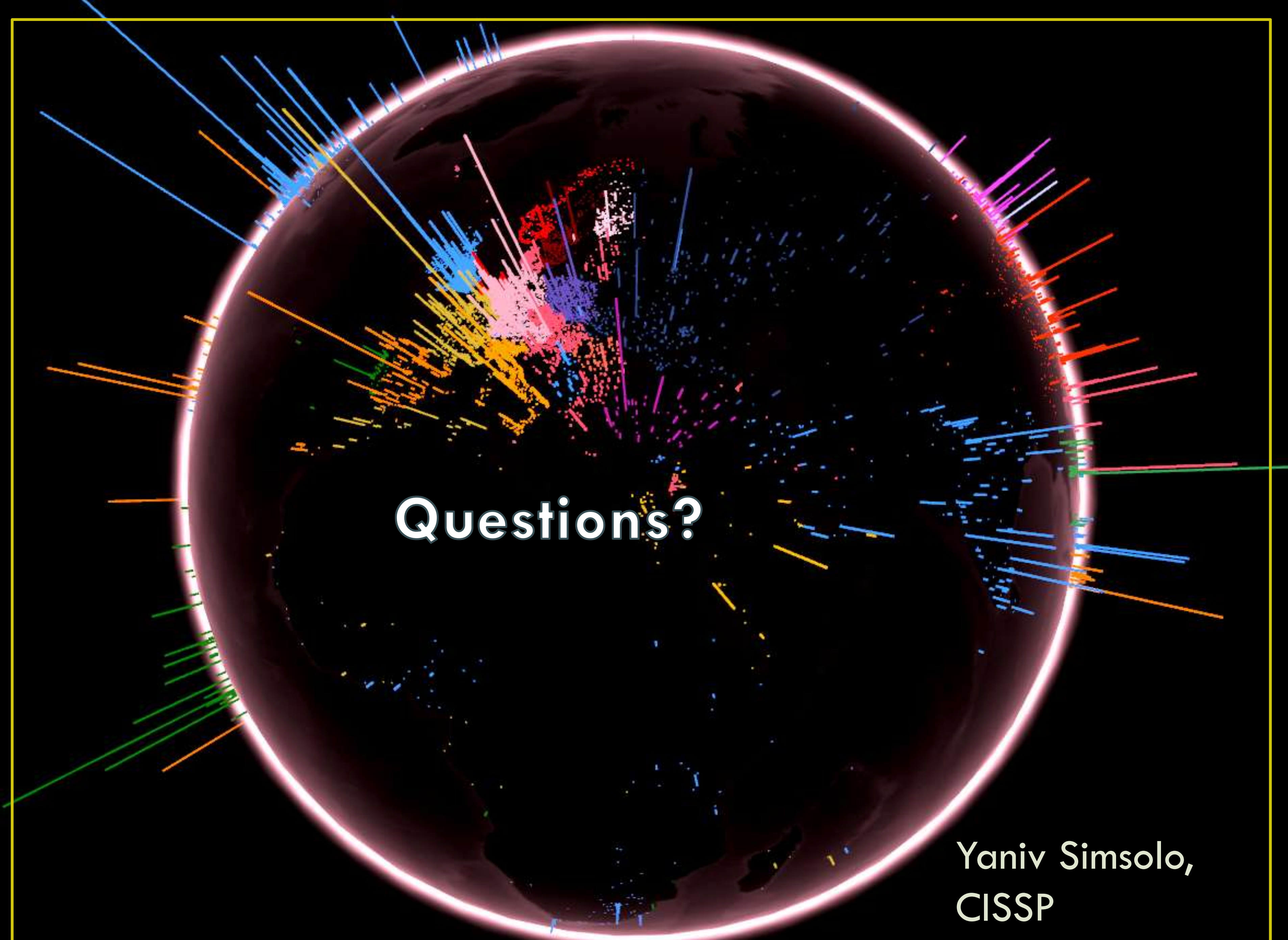
Summary, Hackers Hat

- Forget the payload
- Find the needle in the haystack
- Craft a specialized attack against “the needle”

Summary, Organizations Hat



- Do not concentrate on the payload
- Do not concentrate only on perimeter protection
- Find the needle in the haystack
- Craft specialized security defenses to protect “the needle”
- Do not deter, there is no escaping of in-depth security.



Questions?

Yaniv Simsolo,
CISSP