RSA Conference 2016
San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: TECH-W04

Applying Top Secret and Military Network Grade Security in the Real World

Dan Amiga
CTO & Co-Founder
Fireglass
@DanAmiga

Dor Knafo
Security Research Team Leader
Fireglass
@DorKnfao

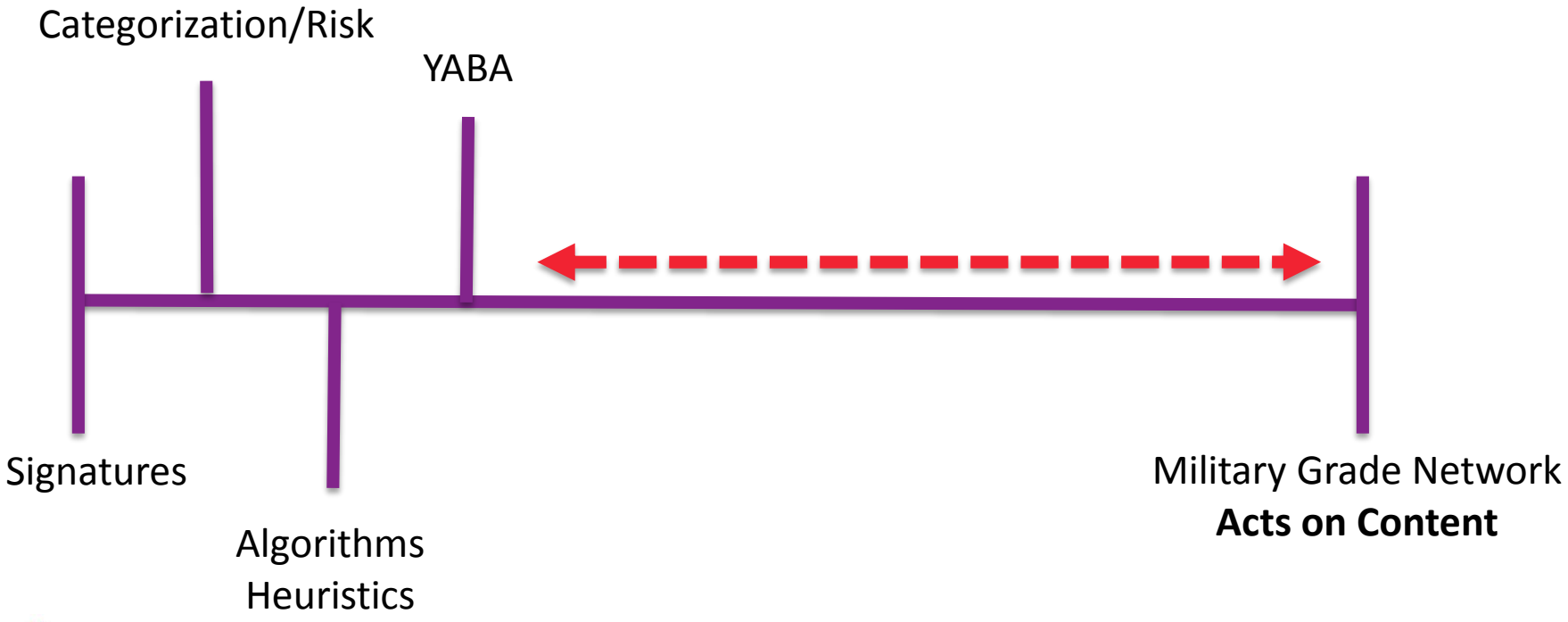
Agenda

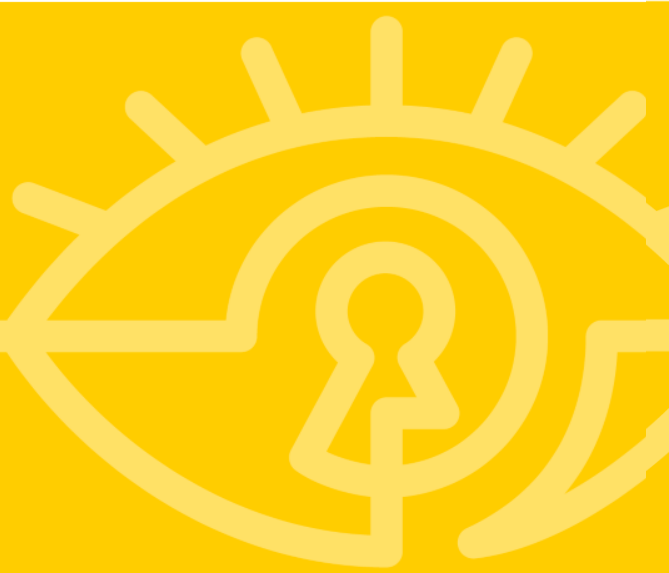
- The fundamental gap
  - Military vs Private Sector
- Challenges & Solutions
  - Networking
  - Internet Connectivity
  - Web Applications
  - File Content
- Summary

Reality Check Matrix

	Private Sector	Military
Adversaries	Crime, Activists Competitors Foreign Governments	Foreign Governments
Operating Mode	Productivity First Limited Budget	Security First Zero Tolerance
Solutions	Commercial Mostly	Commercial & Custom

Decision vs Action



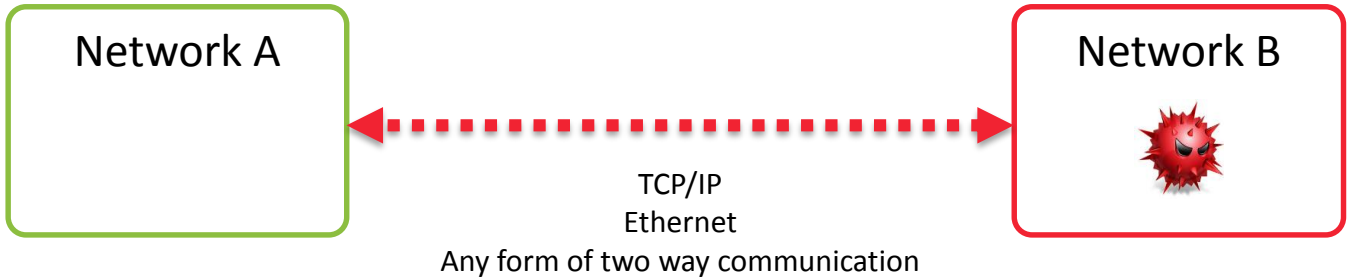


Networking

Data Transmission

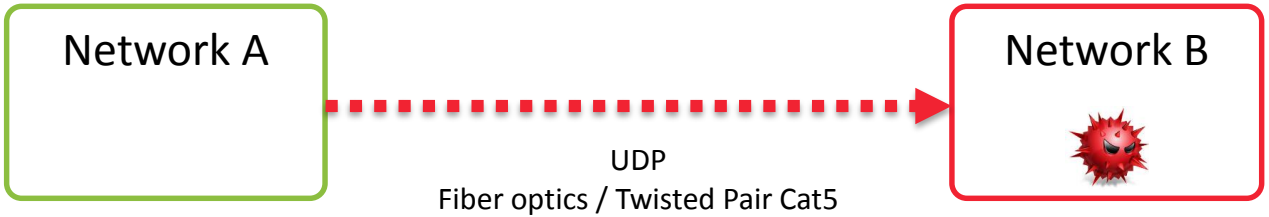
The Data Transmission Challenge

- Problem definition
  - How to transmit data from A to B?
  - Connectivity implies attack surface all the way from packet manipulation, malicious response data or protocol vulnerabilities



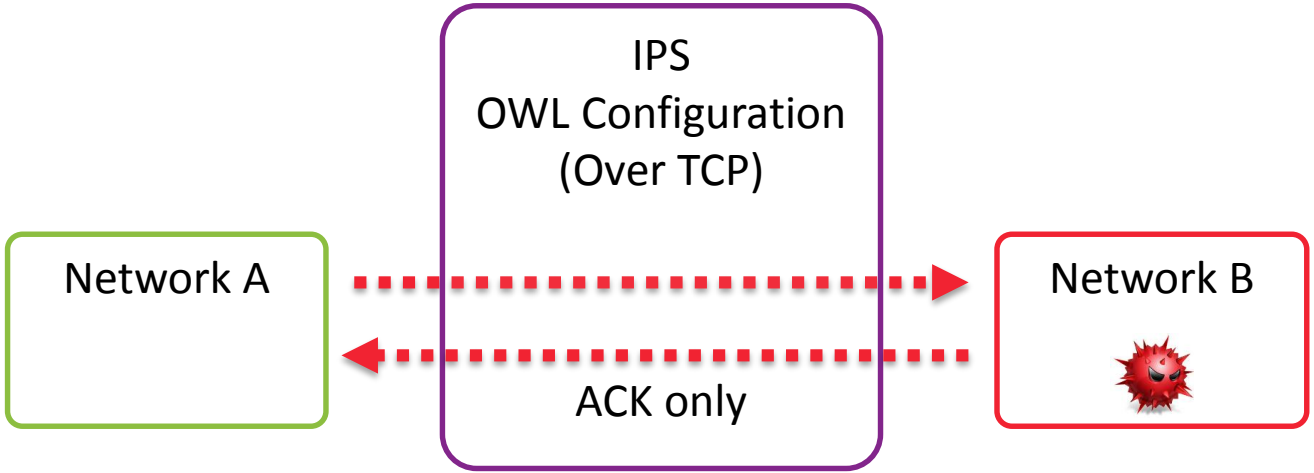
Physical Solution

- Implement a hardware based one way link
  - Modified Ethernet Cable or Fiber Optics
- Significantly reduces attack surface
- Not always feasible and productive



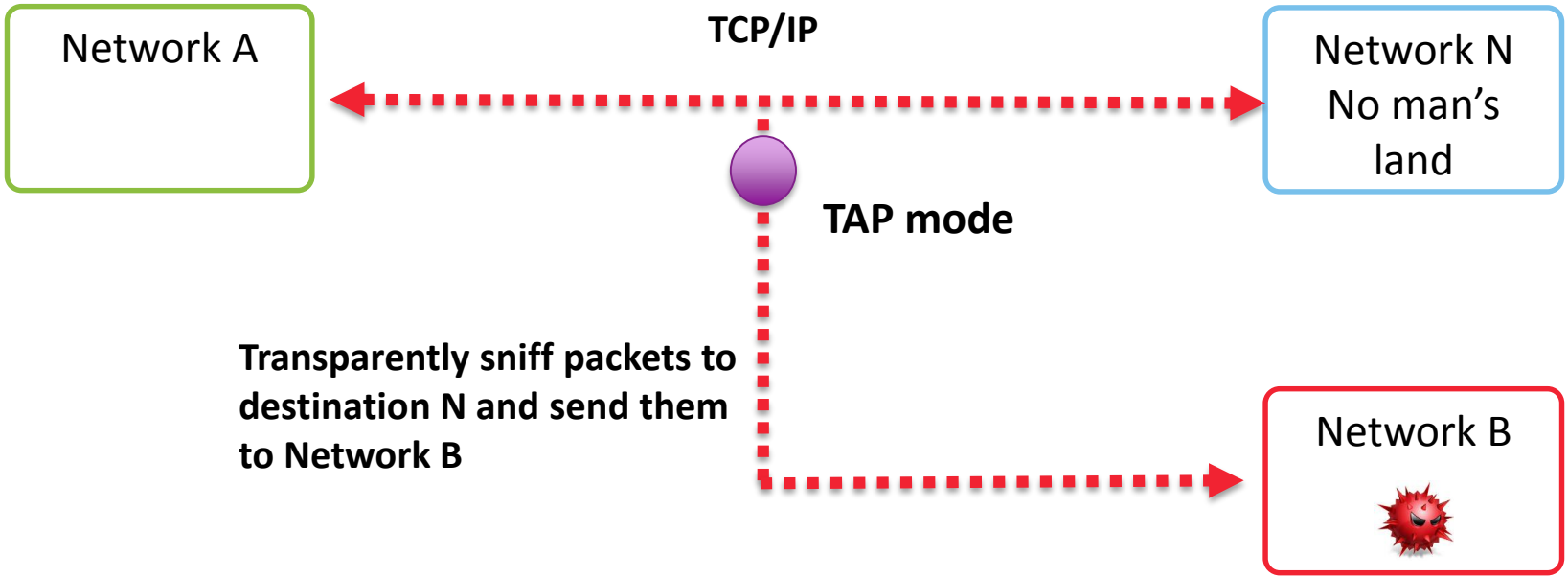
Software Based One Way Link

- Leverage IPS - response size set to zero and allow only ACKs



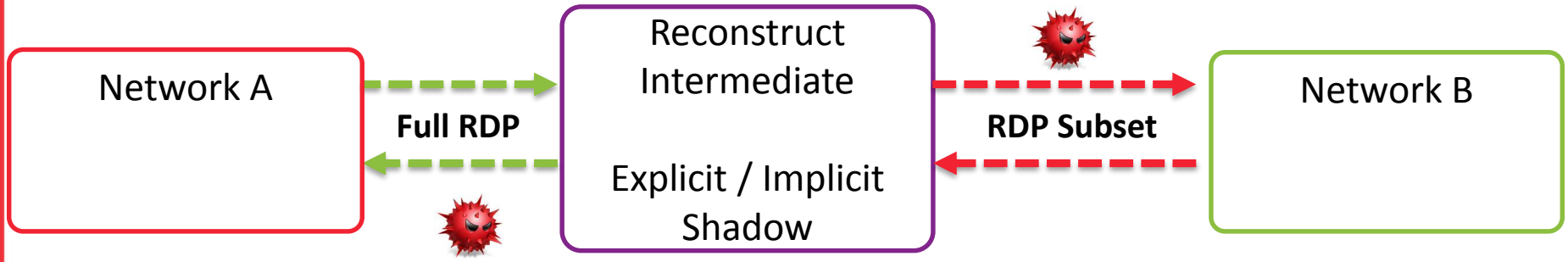
TAP Mode

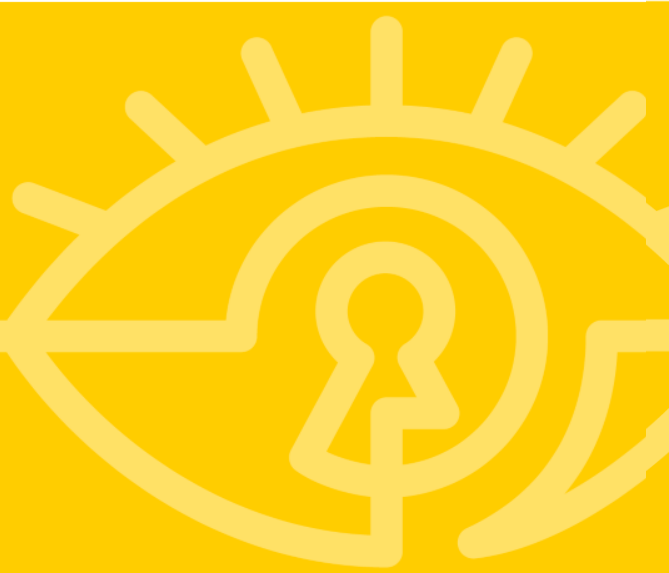
- Leverage promiscuous mode



Enforcement by Reconstruction

- Protocols can be Big & Complex or Proprietary - Hard to analyze.
- Move from open systems to a closed well defined system
- Move from inspection to reconstruction (e.g. HTTP, RDP)





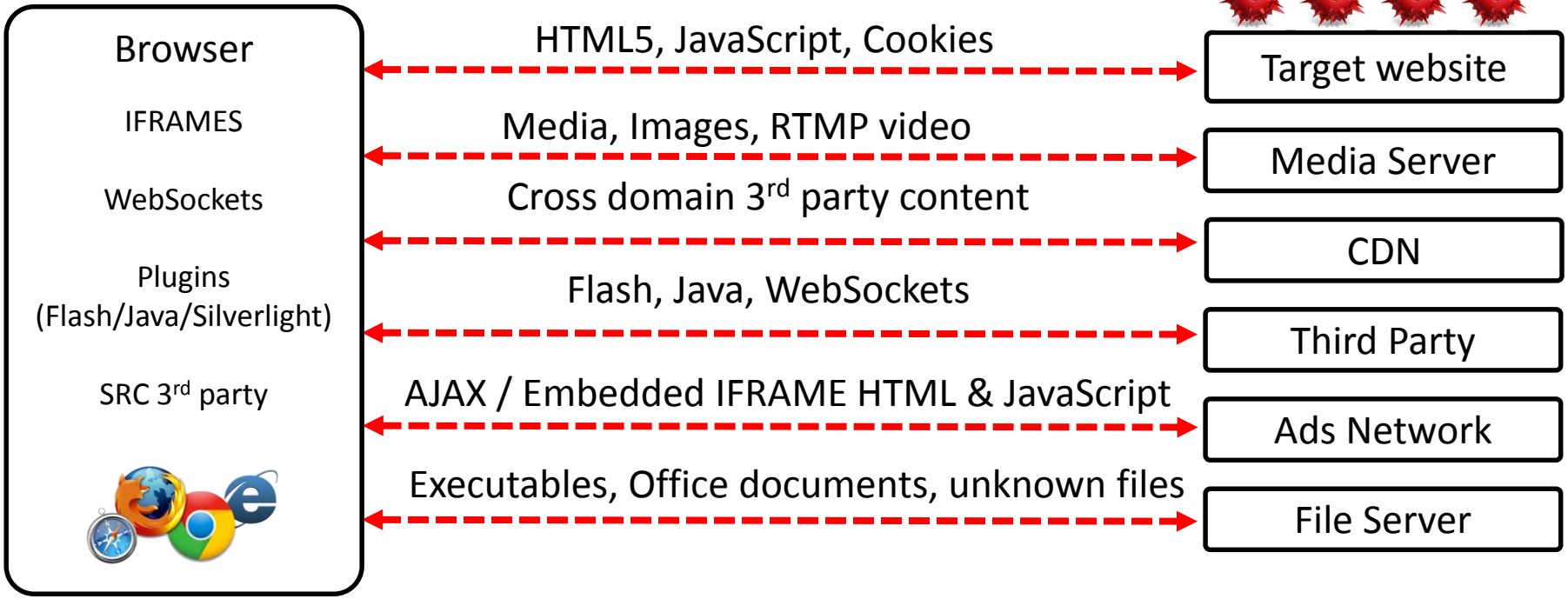
Internet Connectivity Challenges & Solutions

Internet Access Challenge

- Browsing in the #1 productivity tool
- Cannot rely on the (fairly good) browser security model
  - E.g. Chrome sandboxing model

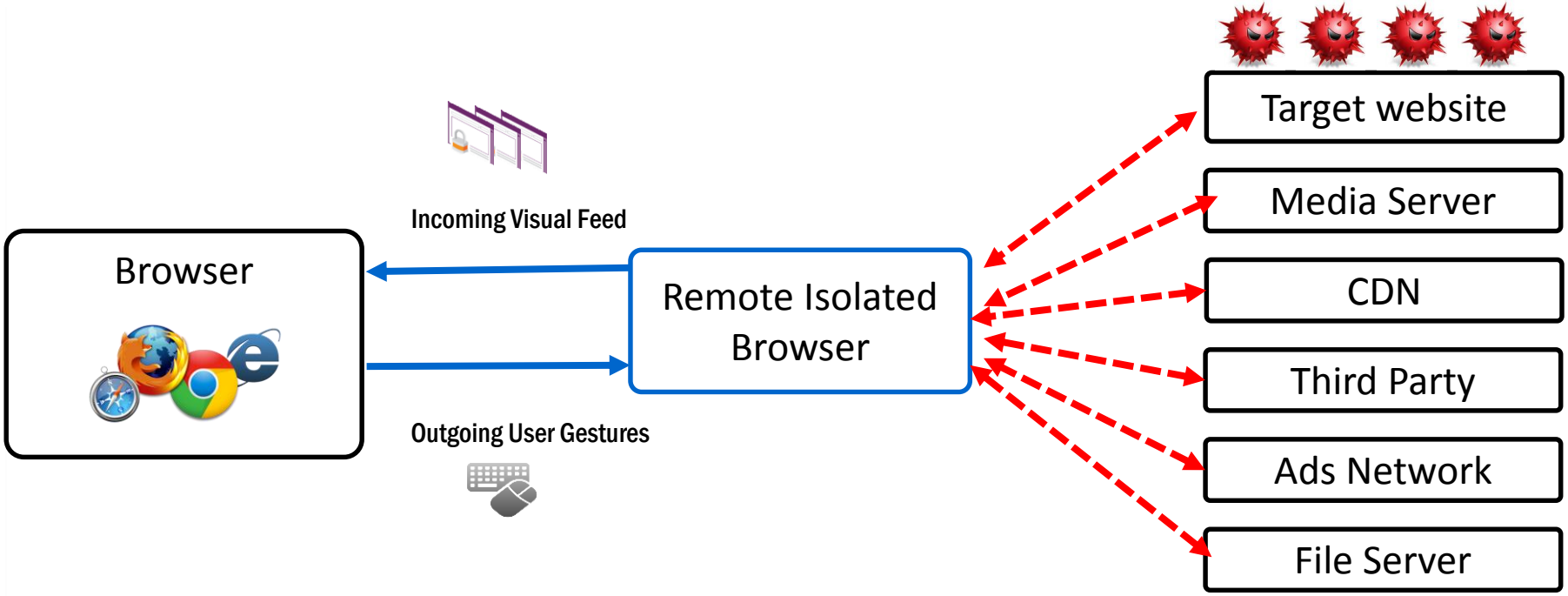
Exploits	Phishing	Fraud	Files	Data Theft	Water holing	Malvertising
Malicious Toolbars	Data Theft	Spearing Emails	Plugins	Legacy	Certificates	OWASP

Browsers & HTTP….

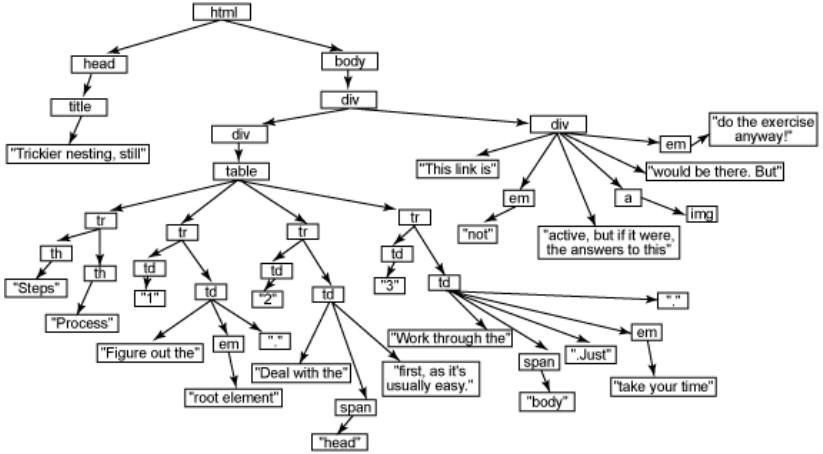


fireglass

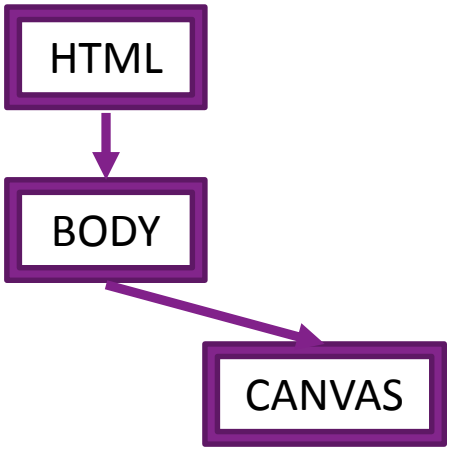
Remote Isolation



Remote Isolation Technical



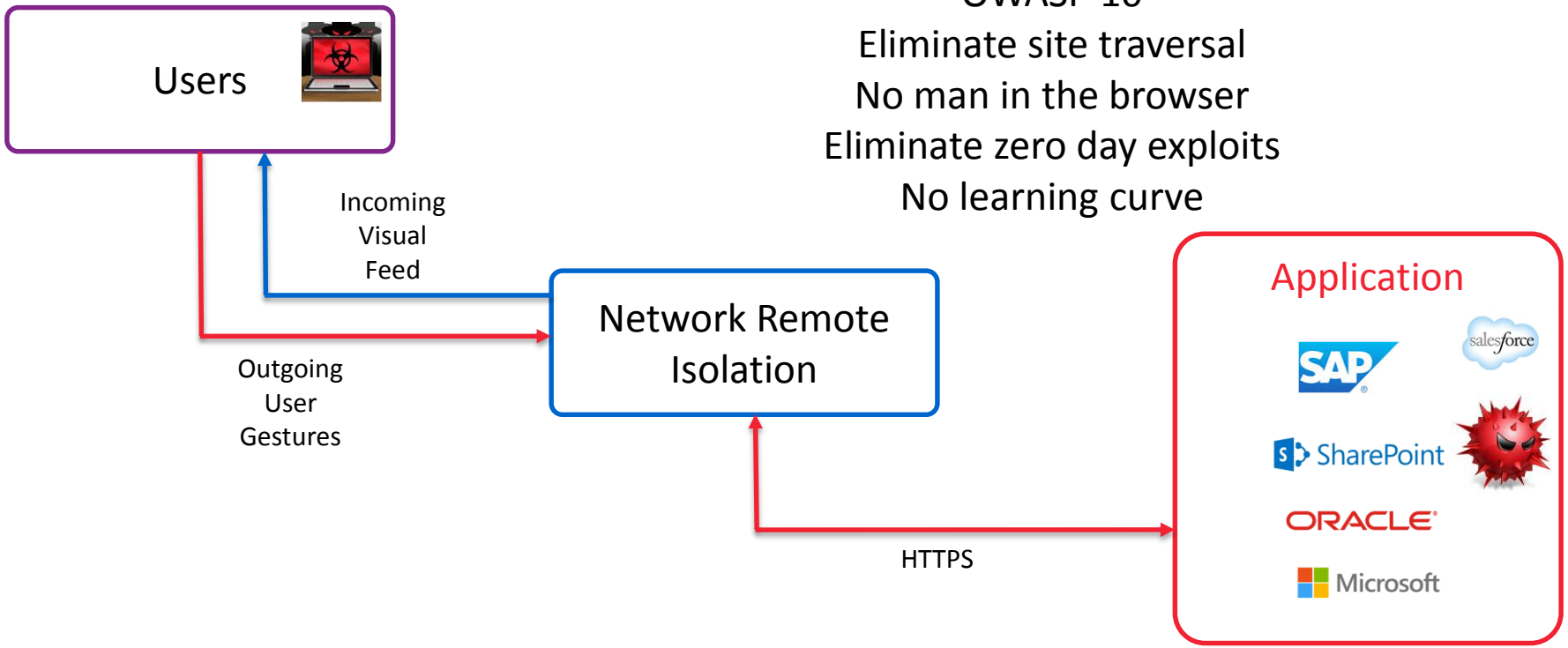
Without

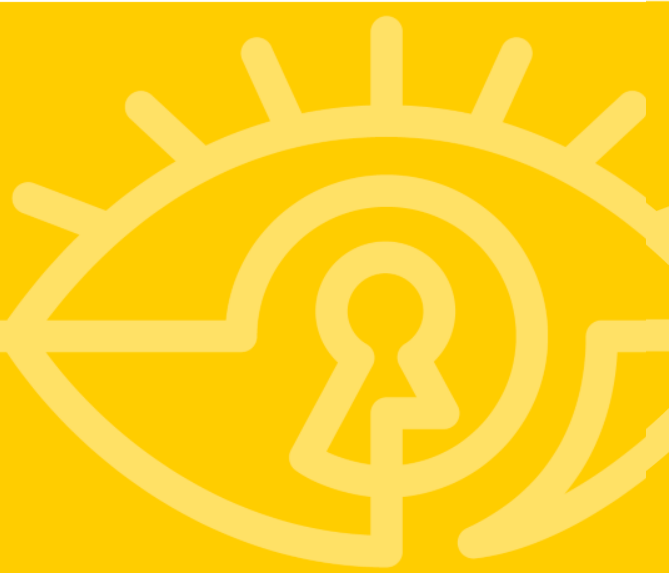


With

Web Application Isolation

OWASP 10
Eliminate site traversal
No man in the browser
Eliminate zero day exploits
No learning curve





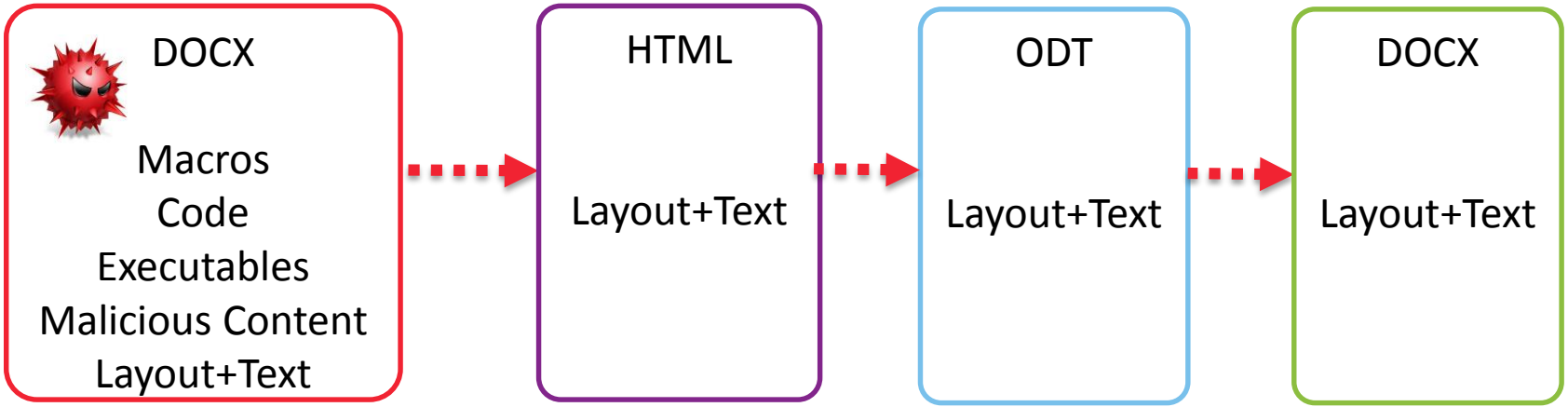
Files…
Challenges and Solutions

The Files Challenge :-)

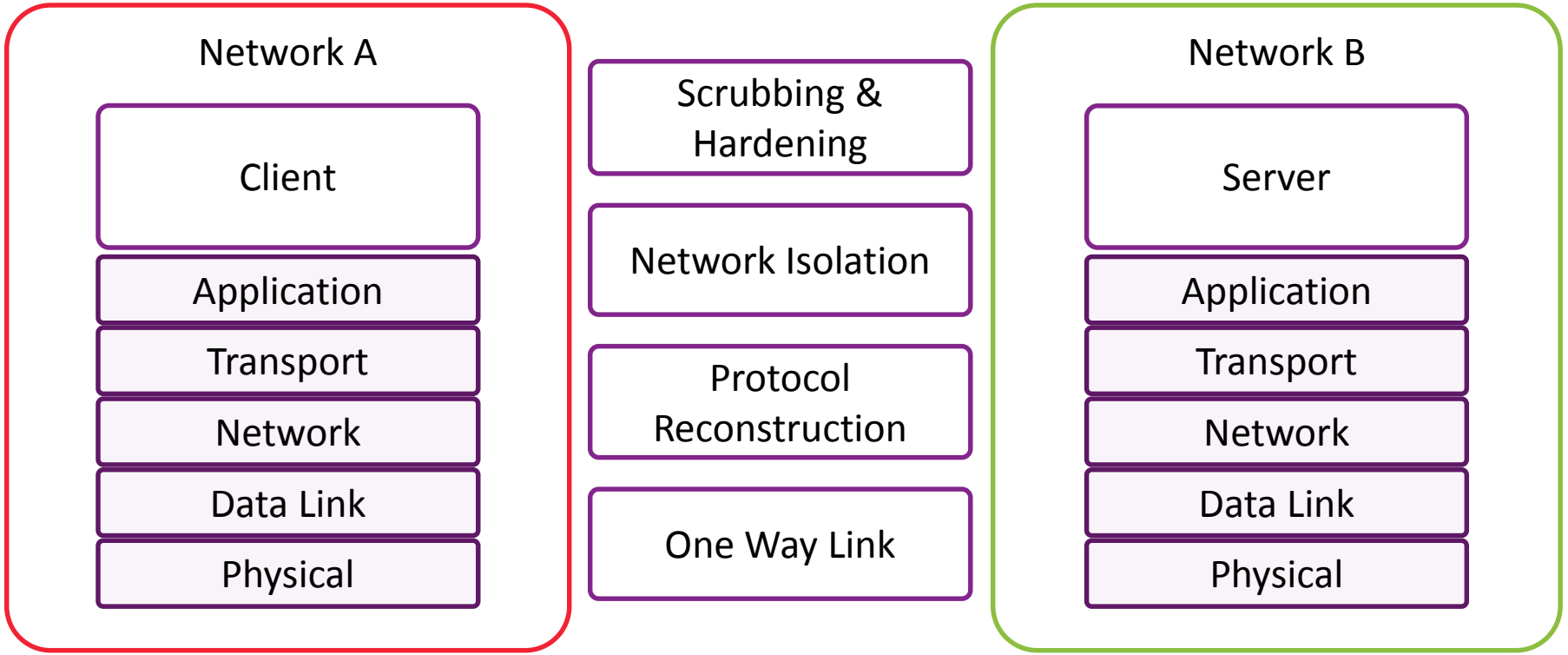
- Executables
  - Remote Isolation (temporary VDI)
  - Sandboxing
- Content (Office)
  - Remote Viewing
  - Reconstruction & Sanitization

Reconstruction & Sanitization

- Multiple Converters
  - Sanitization, SDK based, combined with OWL.



Summary - Architecture



Summary – Commercial Applicability

- New approach discussed – Zero Tolerance
- Touched both network and application level scenarios
- Call for action
  - Identify critical intersection points, actors and systems
  - Understand vendor & solution pros and cons
  - Search for new alternatives from emerging providers
  - Look for the security & productivity sweet spot

RSA Conference 2016
San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: TECH-W04

Applying Top Secret and Military Network Grade Security in the Real World

Dan Amiga
CTO & Co-Founder
Fireglass
@DanAmiga

Dor Knafo
Security Research Team Leader
Fireglass
@DorKnfao