Research & Innovation

Building an effective “Triumvirate” for Cybersecurity

How Academia, Government, and Industry work together to solve the most challenging security problems in cyberspace

“Inevitable” New Threats

300K apps available in 2010 → 2M in 2012

Connected devices will outnumber people by 2014

2011 – 2012 phishing attacks up 87%

Pace of Technology

Global Cloud traffic accounts for 2/3 of total Data Center traffic by 2016

2012-2013 14% y/y increase vulnerabilities and threats

Pace of Adoption

2014 Cisco security researchers found that malicious traffic was visible on 100 percent of the networks sampled

IoT grows to multi-billion $$ market by 2020; Billions of connected things

Average cost of breach rose to >$5 million (US) in 2014

Threat Landscape is Rapidly Evolving

Artificial Intelligence CoE

By 2017, 75% of end point related breaches from mobile apps

Cisco’s Country Digitization Acceleration (CDA) strategy is a long-term commitment to a partnership with national leadership, industry and academia to deliver real outcomes faster and more effectively.

- Accelerate the national digitization agenda
- Drive Initiatives that grow GDP
- Create new jobs & training
- Invest in sustainable innovation ecosystems

Digitaliani – i Pillars

NATIONAL STRATEGIC INFRASTRUCTURES

Italian Digital Agenda to make Italy the most advanced Digital Country in Europe.

DIGITAL PUBLIC SECTOR & SMART CITIES

Accelerate the digitization of Italian PS as per Official Goverrnment Digitization Plan Document & bring great value in enabling a smart, pervasive infrastructure to boost the citizens experience in accessing digital services.

NATIONAL INNOVATION CLUSTER

Safety for Food

S4F aims at introducing a globally adopted platform to support risk prevention and operations in the food market.

IoE Manufacturing

Cisco wants to contribute and accelerate the Italian Government task force for Industry 4.0 and manufacturing digitization.

INNOVATION & EDUCATION

Research and Education

Addressing youth unemployment and capture 176,000 IT professionals job demand by 2020 created by digitization.

Enterpreneurship & Business Innovation

Co-investing in VC and creating the Cisco Innovation Bus, a framework to connect all innovation actors and to ease access to Cisco programs, platforms and resources.

FilieraSicura

Develop a Secure & Trusted Supply Chain for Critical Infrastructure

- Security in the Supply Chain is critically important & highly complex
  - National Security Issue
  - Partnership between Academia, Industry & Government required … can't be solved alone
- Partnership Lead by CINI: National Laboratory of Cybersecurity
  - Eight Leading Italian Academic Institutions
  - Industry partners: Cisco and Leonardo SPA
- >20 Scientific Objectives
- 36 month project with multiple parallel tracks
- Goal - Reference Methodology that can be adopted by Government
  - Securing IT Products Throughout Their Lifecycle and Limiting Software Vulnerabilities
  - Real-time Situational Awareness and Cyber-security for Fog-enabled safety critical infrastructures
  - Securing Industrial Control Systems
  - Develop a pilot environment for demonstration, test, and verification

Cisco - Advanced Security Research Team

Problem Statement

Technological advancement and threat sophistication is accelerating at a pace that threatens enterprise & government function worldwide

Strategy

Cisco's Advanced Security Research initiative insures long-term competitive advantage by incubating advanced security technologies in partnership with Academia, Government, and Industry, that align with Cisco's business objectives and demonstrate differentiated global leadership

Create a collaborative & open innovation engine to solve customer trust & security challenges and drive discovery to practice

Goals

- Gain new / diverse perspective
- Learn from past success & failure
- Understand trends (technology radar)
- Anticipate change & inflection points
- Test hypothesis & verify assumptions
- Practical application in new products, services, and policy
- Objective measures of success

Fueling Innovation

- Collaborative & constructive engagement
  - Encouraging creativity - Defer Judgment
  - Constructive Critique
  - Active Bias Minimization
- Avoiding Intellectual Property issues
  - Clear & Regular Communication
  - Open Source
- Embracing failure as a tool - “Get Radical”
- Rejecting the “Not Invented Here ” mentality
- Applied “Ideation”

Discover -> Define -> Evaluate -> Prototype -> Test -> Iterate

Optimizing for Market Drivers - Prioritizing focus areas

- Developing Sustained Competitive Advantage

  Value (Cost & Performance)

  Time to market … time to adoption

- Leveraging Investment Capital
- Maintaining a Diverse Global Perspective
- Coordination with Government Agencies & Interests
- Addressing Complex, Long-term, & Lasting Problems

USD/GEL 1.7650 1.7660 1.7655 1.7655 1.7655 0.00000.00% 472.40 473.65 472.15
USD/BBD 1.9521 2.0292 1.9906 1.9998 1.9906 -0.0091-0.46%
USD/EGP 6.0793 6.1179 6.0986 6.1052 6.0911 0.00030.00%
472.40 473.65 472.15
USD/PYG 4339.40 4540.00 4439.70 4439.70 4429.95 5.250.12%
USD/KHR 4009.00 4079.00 4044.00 4044.00 4023.95 2.000.05%

ID Mkt Trend - > Security Impact - > Research Area -> Build Centers of Excellence

Research Program Strategy

Trend	Security Impact	Research Area	Funded Projects
Cyber-physical systems (IoT/IoE)	Endpoints sense and control real-world with real-world implications but have limited resource capability for security.	• Lightweight endpoint integrity • Lightweight security and crypto • Endpoint and vulnerable device protection • Privacy / Data Protection	• VT (Schaumont), UNC (Reiter), VU (Bos) • Waterloo (Aargaard) • • INRIA (Cunche), VT (Park)
Cloud Computing and Virtualization	• System integrity and data provenance, security and privacy • Virtual chain of trust	• Data provenance • VM / Cloud Workload integrity • Privacy / Data Protection	• • Cisco (WL), Cisco (ARTIM) • UCB (Wagner), INRIA (Imine)
Privacy / Information Hiding	• Hard to detect compromise • Difficult forensics	• IoC discovery / Data Analytics • Enhanced Threat Telemetry • Insider Threat	• Delaware (Cotton), Purdue (Xu) • Cisco (ETTA) •
Compute Advances	• Crypto vulnerable • Compute advances enhance security and compromise detection	• Post Quantum crypto • Crypto Robustness and Transparency • Heterogeneous Computing	• Maryland (Katz) • Penn (Heninger), Maryland (Dachman) UCD (Su), Weimar (Lucks) • Penn (Heninger)
Software Defined Networks	Maintain system integrity/security (vulnerability and strength)	• Software, Process, and System Integrity • Securing SDN	• Indiana (Camp) •
Agile / DevOps / Continuous Deployment	Maintain system security assurance through continuous software changes	• Software, Process and System Integrity • Continuous security assurance/compliance • Crypto Robustness and Transparency • Insider Threat	• UCSB (Sherwood), • W&M (Poshyvanyk) • •
Increasing bad actor sophistication	Broader infiltration and increasing impact of malware	• Resilient / Adaptive Systems • Privacy / Data Protection • Automated ASIC verification • Insider Threat • Supply Chain Security	• WFU (Fulp), W&M (Sun), BU (Goldberg) • • UF (Mishra), UF (Bhunia), UF (Forte) • • CINI (Italy)

Example: Proposed Research Additions - CY17

- Threat Mitigation

  Insider Threat

  Active network threat mitigation

  Disrupt risk or cost/reward models supporting threat actors

  Improve attribution to increase risk for threat actors

- Advanced Cryptography

  Entropy testing (including system and virtual environments)

  Crypto Implementation/Development Agility

  Lightweight Cryptography (IoT)

- Analytics & Privacy

  Transfer Learning: Leveraging data from one environment to create more accurate machine learning models for another

  Imperfect Ground Truth: Quantifying the effects of noisy labels on problems in the security domain

  Malware reuse and mutation prediction

  Privacy

- Platform & Software Integrity

  Virtualization/Cloud Integrity; Trust Chaining, Run-time integrity

  System Integrity (including IoT systems)

  Continuous Deployment/DevOps Security Assurance

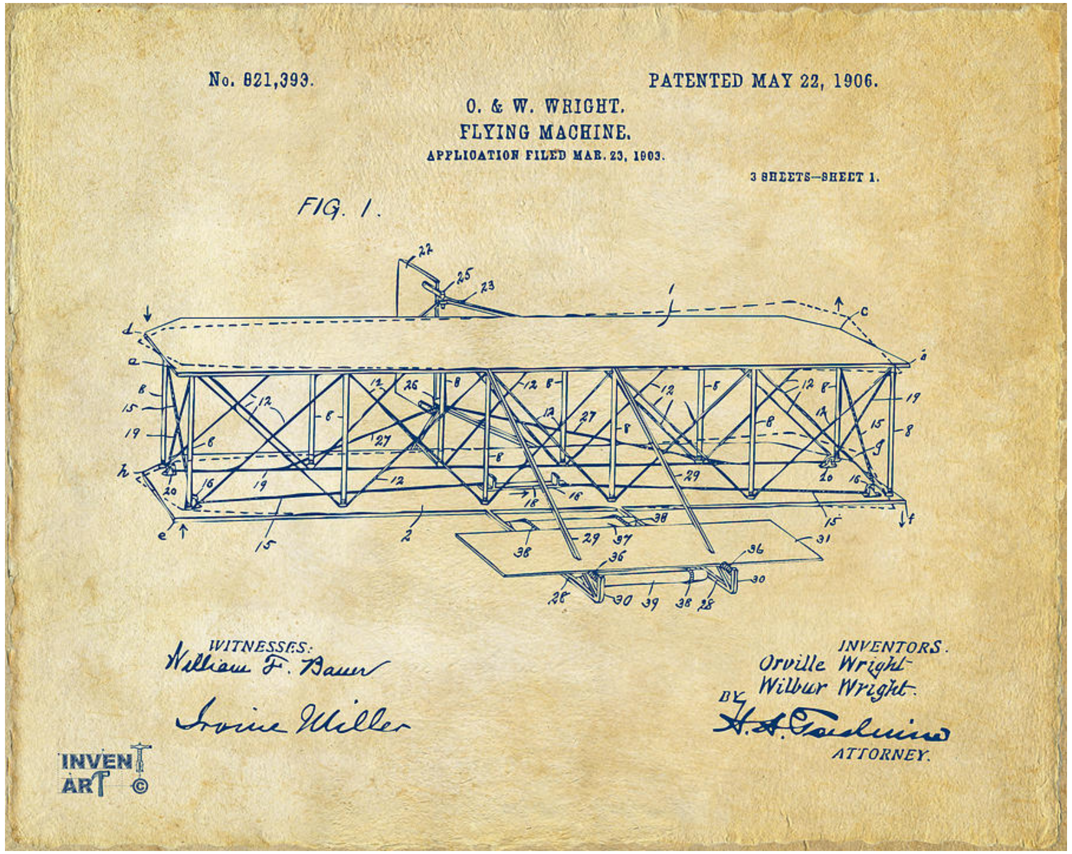
Fail Fast … Fail Forward

- Rapid prototyping to test ideas
- Identify improvement areas
- Iterate with forward motion
- Define metrics which encourage risk taking, creative problem solving, and don't discourage or punish failure!

Jane McGonigal - keynote speaker at the World Innovation Forum, '12

Driving Discovery to Practice

- Practical Application … start by defining the problem together
- Early Involvement & Investment = Buy-In
- Focus on Recognized Problems
- Tech Transfer on Two Feet
  - Internships
  - In-Kind Contribution
  - Residency



How do we Measure Success?

- **Ideation & Tech Transfer** - Exploration, experimentation, prototyping, beta testing, verification (Breadth & Depth of investments)
- **Fail / Fast / Forward** - examples include advancing knowledge through risk taking, rapid prototyping, experimentation, iterative learning
- **Customer/Partner Engagement** - Investment level
- **Industry Influence**
- **Education**
- **Recruitment**

Thank you.

CISCO

Back-up Slides

Research Focus Areas

- Advanced Cryptography
- Platform & Software Integrity
- Analytics & Privacy
- Threat Mitigation

Advanced Cryptography

Area	Description	Lead	PR	Term	Prirty	Role	Value
Quantum Resistant Crypto	Establish and standardize cryptographic algorithms that maintain security even with Quantum computing attacks.	McGrew		M	M	Leader	Customer trust
Protect IoT Secrets	How to seal and secure secrets for IoT devices that may not support secure storage; information about a specific system state decryptable only from the same state.	Robert		N	M	Leader	
Quantum Key Dist	Investigate utility, feasibility, practical applicability of QKD.	McGrew		M	L	Observer	Show limitations
Homomorphic Crypto	Develop and understand the limitations of homomorphic encryption applied to operations on encrypted data.	McGrew		Fully (L) Part (M)	H	Guide	Differentiation, Customer trust
Low Power Crypto	Cryptography for low power devices (IoT).	McGrew		N	M	Lead	Differentiation
Crypto Innovation	Work with industry leaders to investigate new crypto systems that improve security and efficiency.	Greg A		N	M	Lead	Differentiation
Robustness and Transparency	Need: algorithms, protocols, and implementation techniques that are simple, robust, and can be transparently verified as correct	McGrew		L	H	Lead	
Data Oriented Crypto	Architectures for encryption and signatures of persistent data, to promote verifiable trust of communicated data	McGrew		M	M	Explore	

Analytics

Area	Description	Lead	PR	Term	Prirty	Role	Value
Anonymity & Privacy	Approaches to maintain anonymity, confidentiality, and privacy when performing data mining.			M	H	Lead	Customer Trust
Cloud Security	Provide measurements and controls to monitor, manage and secure cloud workloads and data.	Broberg		N	H	Lead	Customer Trust
Mobile & IoT Security	Techniques to detect malware injection & C2.	Bieda		L	M		Differentiation
IoC Discovery	Analyze large, unstructured data sources (e.g., log files, config files, temporary files, flows) for IoCs (Indicators of Compromise)	Seagle		N	M	Guide	
Side-channel Malware Detection	Use power and signal analysis to detect if malware is operating in a device.	Rich		L	H	Lead	Differentiation
Insider Threat	Methods to predict, detect, and mitigate insider threats.	Bieda		L	H		
Enhanced Threat Telemetry	Use additional telemetry (SALT, 1st packet, etc.) to determine App & IoC in the presence of encryption	McGrew		N	H	Lead	Differentiation

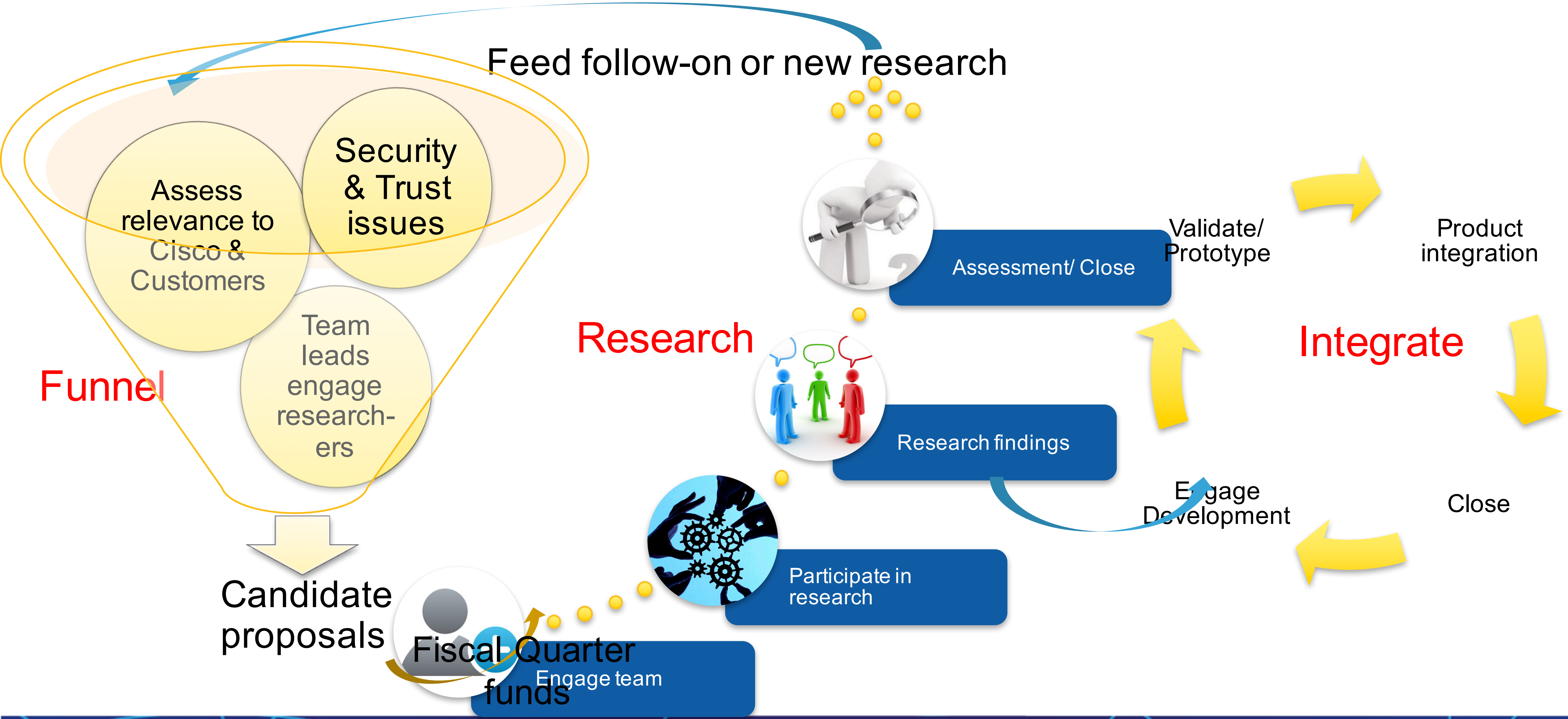
Integrity (Platform & Software)

Area	Description	Lead	PR	Term	Prirty	Role	Value
Low Power Integrity	Find algorithms that maintain integrity even with Quantum computing attacks. Current integrity approach with LDWM (Lamport, Diffie, Winternitz, and Merkle) could lead to a near term application for integrity and is already implemented for integrity in some Cisco products.	McGrew		M	M	Guide	Prevent Disruption
Software/Process Integrity	Introspection that identifies in-memory indicators of compromise.	Rich		M	H	Lead	Customer Trust
VM/Cloud Workload Integrity	Measure, manage and report the integrity of virtual machines running in cloud (public/hybrid) environments. This work includes managing integrity of Network Function Virtualization	Robert		N	H	Lead	Customer Trust
Automated ASIC verification	Provide rapid and scalable mechanisms to verify ASICS as-built.			M	M	Lead	Differentiation
Formal Code Verification	Methods and technologies to perform formal code verification across any language and for vulnerabilities from code standards to logic errors.	Rich		L	H	Observer (strive to lead)	Customer Trust

Threat Mitigation

Area	Description	Lead	PR	Term	Priorty	Role	Value
Recover from Destructive Attacks	Methods/technology to recover from attacks that result in damaged/diminished infrastructure. This may include a roll-back to a known good state but also considers network behaviors of synchronized relationships between neighbors. Related consideration is determining when a device or system of devices in recovery is "trustworthy".	Chris		L	M	Lead	Differentiation Consumer Trust
Protect Vulnerable Components	Methods and technology to protect systems that are known to be vulnerable even if those systems cannot be upgrade/mitigated. This protection could be temporary until a patch or replacement, or permanent.	Seagle/Bieda		M	H	Guide	Consumer Trust?
Resistant/Adaptive Systems	Methods to improve system's resistance to attacks and adapt if attacks are detected. Cisco emphasis should be how to build adaptive networks that mitigate the impact of attacks.	Seagle/Bieda		L	H	Lead/Guide	Differentiation

ASRG Research Process



Feed follow-on or new research

Funnel

Assess relevance to Cisco & Customers

Security & Trust issues

Team leads engage research-ers

Candidate proposals

Fiscal Quarter funds

Research

Engage team

Participate in research

Research findings

Assessment/ Close

Integrate

Validate/ Prototype

Product integration

Close

Engage Development