Educação e Treino para a Cibersegurança e Ciberdefesa:

Edificação de um “Ciber Currículo"

inserido no

Simpósio Internacional 10ºEIN/xºOVL

”*Ciberespaço: Liderança Virtual, Segurança e Defesa na Sociedade em Rede*”

Academia Militar

Amadora, 29 de abril de 2016

Henrique Santos

(hsantos@dsi.uminho.pt)

Centro Algoritmi / Universidade do Minho

Sumário

- Introdução
  - Haverá uma “Ciência da CiberSeg”?
  - Bases de um currículo
- Profissionalização e Certificação Profissional
- CBK e competências
- Síntese das propostas no âmbito do projeto MN CD E&T
- Conclusões

Haverá uma "Ciência da CiberSeg"?

- A existir deverá permitir criar sistemas seguros, fundamentados em **princípios sólidos** e **leis** que permitam prever as consequências das decisões de desenho e implementação; fortemente apoiado na experimentação (Schneider, 2011)
- A **incerteza** relativamente aos contextos e a **complexidade** dos ciber sistemas "impedem" o desenvolvimento de uma ciência "tradicional" (McDaniel, 2014)
- Projetos como o DeterLab procuram contribuir para uma abordagem mais científica (Benzel, 2011)

Bases de um currículo

- Princípios básicos:
  - Finalidades educacionais (objetivos)
  - Selecionar tópicos e atividades educacionais úteis
  - Organizar as atividades (eficiência)
  - **Avaliar eficácia das atividades**

(Tyler, 1949)

Profissionalização

- Existe uma profissão quando existe (Cox, 2010, p.7):
  - Um Corpo de Conhecimento devidamente estabelecido
  - Um código de ética
  - Algum tipo de **organização profissional** que disciplina, regula, ou controla os atos profissionais e competências
- Profissionalização acontece quando "uma ocupação", ou "tarefa", evolui através de uma qualificação formal (educação, treino e examinação), até à **organização socioprofissional** de suporte (Bullock and Trombley, 1999)

Tipos ou categorias de profissionalização

- Modelos baseados em atributos
- Modelos baseados em processos
- Modelos baseados em poder
- Modelos híbridos

Tipos ou categorias de profissionalização

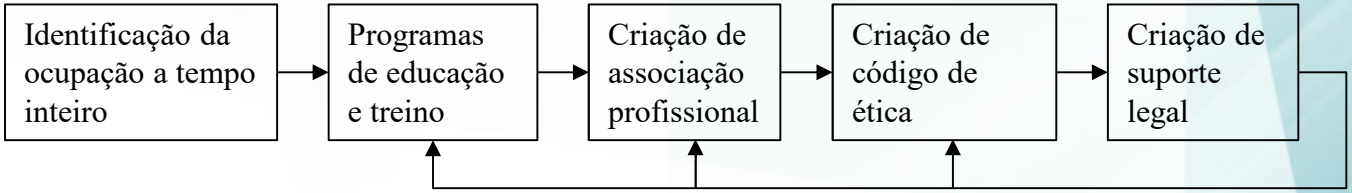
- Modelos baseados em atributos
- Modelos baseados em processos
- Modelos baseados em poder
- Modelos híbridos

- Competências baseadas no conhecimento da área
- Critérios de aceitação perfeitamente conhecidos
- Profissão definida como algo diferenciado de qualquer outra ocupação
- Frequentemente associada a um serviço público

Tipos ou categorias de profissionalização

- Modelos baseados em atributos
- Modelos baseados em processos
- Modelos baseados em poder
- Modelos híbridos

- Perspetiva mais holística
- Assume-se alguma sobreposição com outras ocupações
- Evolução contínua da profissão



Tipos ou categorias de profissionalização

- Modelos baseados em atributos
- Modelos baseados em processos
- Modelos baseados em poder
- Modelos híbridos

- Orientado pelas leis de mercado, para:
  - limitar interferências e valorizar certificações
  - valorizar algum tipo de conhecimento e competências
  - monopolizar serviços

Certificação Profissional

- (apenas) 5 das mais solicitadas/valorizadas
  - Certified Information Systems Security Professional (CISSP) (ISC)^2
  - Certified Information Systems Auditor (CISA) (ISACA)
  - Certified Information Security Manager (CISM) (ISACA)
  - GIAC Security Essentials (GSEC) (GIAC)
  - CompTIA Security+ (CompTIA)

“Carreiras” em Cibersegurança

- Segundo a NICCS:
  - Chief Information Security Officer (CISO)
  - Computer Crime Investigator
  - Computer Security Incident Responder
  - Cryptanalyst
  - Cryptographer
  - Disaster Recovery Analyst
  - Forensics Expert
  - Incident Responder
  - Information Assurance Analyst
  - Intrusion Detection Specialist
  - Network Security Engineer
  - Security Architect
  - Security Analyst
  - Security Consultant
  - Security Engineer
  - Security Operations Center Analyst
  - Security Systems Administrator
  - Security Software Developer
  - Source Code Auditor
  - Virus Technician
  - Vulnerability Assessor
  - Web Penetration Tester

Profissionalização

- O que diferencia estes profissionais?
- Que atos profissionais lhes estão associados?
- Que conhecimento sustenta as competências e como foram validados?

BoK & Competências

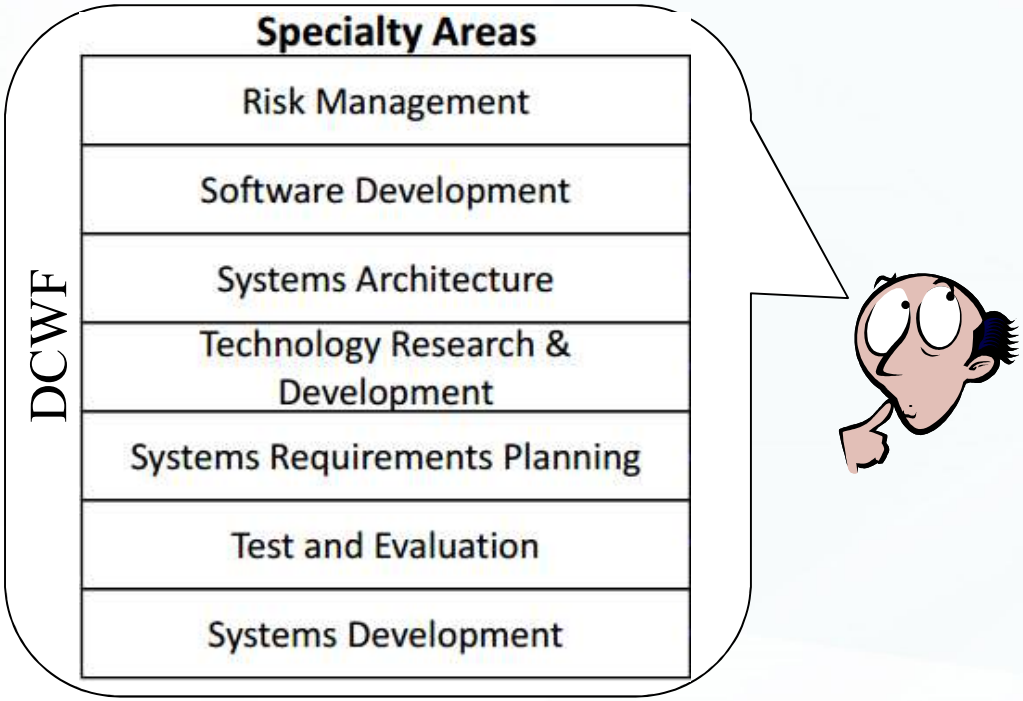
- Crowley identifica 3 percursos principais (grupos de competências)

Technician	Manager/Developer	Auditor/Researcher
Risk Management	Risk Management	Forensic Analysis
Ethics and Legislation	Ethics and Legislation	Legislation and legal proofs
Computer Technology	Software Engineering	Privacy
HR Management	HR Management	Psychology
Test and Development	Test and Development	Standards and Certification
Communication Networks	Access Control	Access Control
	Intellectual Property	
	Procurement	

Crowley, E. 2003. Information system security curricula development. In *Proceedings of the 4th Conference on information Technology Curriculum*

BoK & Competências

- *National Cybersecurity Workforce Framework* (produto da National Initiative for Cybersecurity Education – NICE)
  - Assenta em 7 categorias (profissões/funções) de alto nível, cada uma integrando áreas de especialização, conhecimento e competências



CBK & Competências

- Síntese de um estudo realizado sobre 135 instituições académicas
  - 15 cursos de graduação e 45 de pós-graduação
  - **Maioritariamente ligados a departamentos de Ciências de Computação e Engenharia de Computadores**
  - Vários cursos oferecem (normalmente como opção) disciplinas de SegInfo

Theoharidou, M. et. al., "*Common Body* of *Knowledge* for *Information Security*," IEEE *S*&P, March/April, 2007

CBK & Competências

- … **identifica competências** exigidas pelas organizações, através de propostas de oferta de trabalho (limitadas à SegInfo)
  - *Information Security and HCI*
  - *Computer Forensic Analysis*
  - *Data Base Security and Data Mining*
  - *OS Security*
  - *Malicious Software*
  - *Internet and Cyber Security*
  - *Incident Management*
  - *Hacking*
  - *Cryptography*
  - *Biometrics*
  - *Smart cards*
  - *Auditing (security)*
  - *Data Protection and Critical Infra Structures*
  - *Risk Management*

CBK & Competências

- … e propõe um CBK assente em 10 domínios
  1. *Management and business within Information Systems Security*
  2. *Physical security and critical infra structures protection*
  3. *(Security) Architecture and security models*
  4. *Systems and methodologies for access control*
  5. *Network and telecommunications security*
  6. *OS security*
  7. *Software and applications security*
  8. *Data Base security*
  9. *Cryptography*
  10. *Social, legal and ethical issues*

CBK & Competências

- Modelo curricular proposto por AIS e ACM/SIGMIS também inclui UCs de SegInfo (ACM, 2012):
  - Fundamentos da Segurança da Informação
  - Segurança em Redes
  - Segurança em Computadores
  - Segurança na Internet
  - Ética, Privacidade e Políticas de Segurança
  - Gestão do Risco
  - Auditoria de segurança
  - Crime informático, ciberterrorismo e ciberguerra

Muito embora neste caso não seja absolutamente claro que o painel esteja a considerar explicitamente os riscos relacionados com a segurança, os métodos são em tudo comuns

CBK & Competências

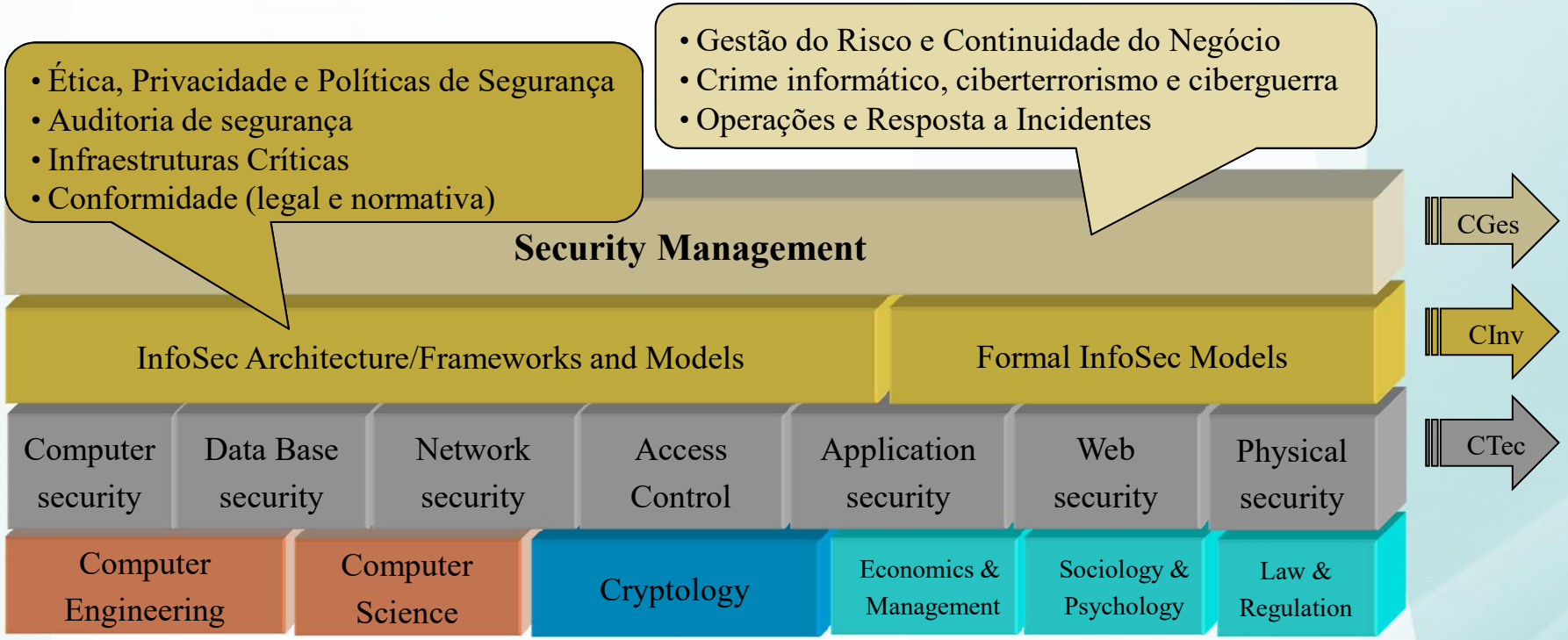
- Grupo de discussão no *45th ACM Technical Symposium on Computer Science Education, 2014*:
  - **Debilidades do sistema educativo, a todos os níveis, para suportar a educação – em particular falta de PhDs e um corpo docente adequado**
    - Nível do ensino superior: dos 73 cursos analisados apenas 5 estão associados a departamentos específicos (maioria deriva de formações em TIC)
  - Justifica-se o esforço ao **nível da pós-graduação/mestrado**
  - **Diversificar experiências e apostar no desenvolvimento da "Ciência da Cibersegurança"**
  - Necessário o envolvimento de todos os setores
  - Atendendo à falta de maturidade da área ainda não será oportuno avançar com referenciais curriculares

CBK & Competências

- Grupo de discussão no *45th ACM Technical Symposium on Computer Science Education, 2014*:
  - Reconhece os tópicos identificados pelo grupo de trabalho ITiCSE
    - Fundamentos da Segurança da Informação
    - Criptografia
    - Ética em Segurança da Informação
    - Políticas de Segurança
    - Análise Forense Digital
    - Controlo de Acesso
    - Arquiteturas e Sistemas de Segurança
    - Segurança em Redes
    - Gestão do Risco
    - Ataques/Defesa
    - Engenharia de software seguro

Currículo para SegInfo

- Modelo curricular



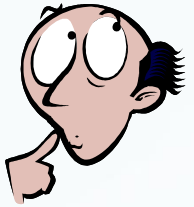
[Yasinsac, 2001] (adapted with [Theoharidou, 2007] e [Santos, 2013] e [McGettrick, 2014])

Currículo para SegInfo

- Treino e/ou educação
  - Treino: desenvolvimento de competências (como fazer) – relevante para as organizações
  - Educação: desenvolver conhecimento, capacidade crítica e capacidade de resposta pró-activa (porquê) – relevante para as Universidades e instituições de investigação
    - Graduada – conhecimento fundamental
    - Pós-graduada – desenvolvimento do conhecimento

Atividades pedagógicas

- Educação (CS/CD)
  - Multidisciplinar; sistema aberto… diferentes estilos de aprendizagem!
  - *Critical Thinking, PBL, Cases, Learning Communities*,…
- Treino (CS/CD)
  - Seleção e preparação de materiais (crítico)
  - *Active Learning* e *Collaborative/Cooperative Learning*
  - Competições tipo CTF ou CDC



Educação

- Que métodos são mais eficientes? Em particular para determinadas competências…
  - Como se ensina a competência para "reconhecer e responder a comportamentos complexos e emergentes"?
  - Como se ensina a capacidade para "entender a forma de pensar do adversário"?
  - Como se ensina a "manipular a incerteza e a ambiguidade"?
  - …

Síntese das propostas no âmbito do projeto MN CD E&T

- Currículos dos mestrados: abordagens híbridas
  - Competências → tópicos e
  - Tópicos → competências
    - Diferentes visões
- Competências fortemente ligadas às necessidades da NATO
  - Alinhamento com *frameworks* de competências e CBK existentes não é fácil
  - Focado em competências técnicas e de gestão/operação
- Projeto possível; avaliação será fundamental para a validação

Conclusão: profissões em SegInfo

- Ainda por realizar o esforço de organização
- Conduzido pelos próprios profissionais
- Mas várias iniciativas empenhadas:
  - CISSE – *Colloquium for Information Systems Security Education*
  - CT 11 do IFIP, em particular o *Working Group 11.8 on Information Security Education*
  - CAEIAE (*Centers of Academic Excellence in Information Assurence Education*); NSA e Homeland Security

Conclusões: geral

- A SegInfo é uma actividade multidisciplinar
- As diferentes organizações têm interesses **comuns** e **diversos**, mas a colaboração é essencial!
- É desejável unificar os CBKs, criando um referencial único… e desenvolvendo a "Ciência da CiberS/D"
- Não há (ainda) experiência suficiente para avaliar eficiência dos métodos de aprendizagem

Obrigado pela vossa atenção.
Questões?

Bibliografia

- ACM (2012). "The 2012 ACM Computing Classification System — Association for Computing Machinery." Retrieved October, 2012, from http://www.acm.org/about/class/2012.
- Armstrong, C. J., H. L. Armstrong, et al. (2007). "Mapping information security curricula to professional accreditation standards." 2007 IEEE Information Assurance Workshop: 30-35.
- Conklin, A. (2006). Cyber defense competitions and information security education: An active learning solution for a capstone course. 39th Annual Hawaii International Conference on System Sciences (HICSS '06), University of Texas at San Antonio, USA, IEEE.
- Crowley, E. (2003). Information system security curricula development. Proceedings of the 4th conference on Information technology curriculum. Lafayette, Indiana, USA, ACM**:** 249-255.
- Hoffman, L., D. Burley, et al. (2012). "Holistically Building the Cybersecurity Workforce." Security & Privacy, IEEE **10**(2): 33-39.
- Hoffman, L. J., T. Rosenberg, et al. (2005). "Exploring a national cybersecurity exercise for universities." Security & Privacy, IEEE **3**(5): 27-33.
- Lee, C. P., A. S. Uluagac, et al. (2011). "The Design of NetSecLab: A Small Competition-Based Network Security Lab." Education, IEEE Transactions on **54**(1): 149-155.
- Mullins, B. E., T. H. Lacey, et al. (2007). "How the cyber defense exercise shaped an information-assurance curriculum." Security & Privacy, IEEE **5**(5): 40-49.
- Pfleeger, S. L., C. Irvine, et al. (2012). "Guest Editors' Introduction." Security & Privacy, IEEE **10**(2): 19-23.
- Theoharidou, M. and D. Gritzalis (2007). "Common body of knowledge for information security." Ieee Security & Privacy **5**(2): 64-67.
- Yasinsac, A. (2001). Information Security Curricula in Computer Science Departments: Theory and Practice, Department of Computer Science, Florida State University.

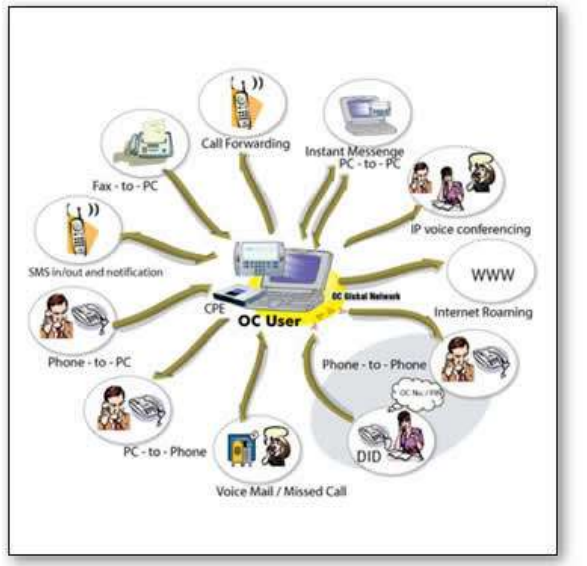
Certificação Profissional

- EC-Council Certifications
  International Council of Electronic Commerce Consultants
  - IT Security Professional Certifications
    - Certified Ethical Hacker (CEH)
- Certified Information Privacy Professional (CIPP)
  International Association of Privacy Professionals (IAPP)
- Symantec Certifications
- Professional in Critical Infrastructure Protection (PCIP – formerly CCISP)
  Critical Infrastructure Institute (CII)

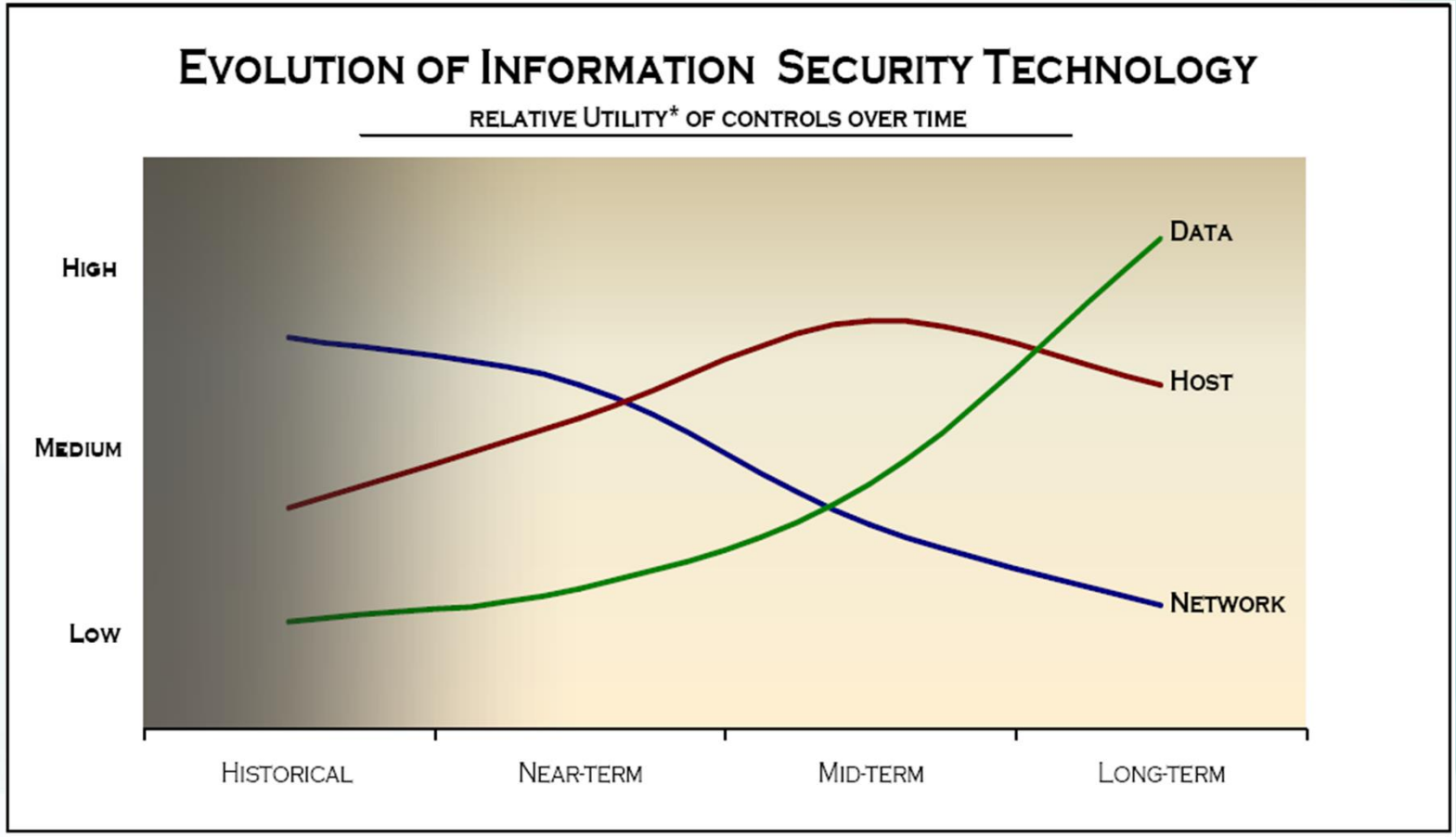
Evolução da SegInfo

- Evolução dos Sistemas Informáticos (≈50 anos)
  - Poucos Centros de Computação isolados
  - Sistema em t*ime-share*
  - As **redes** de comunicação de dados (sistemas distribuídos)
  - A **computação pessoal**
  - A **computação ubíqua** e a convergência de tecnologias
  - **IoT**

Flexibilidade
Insegurança

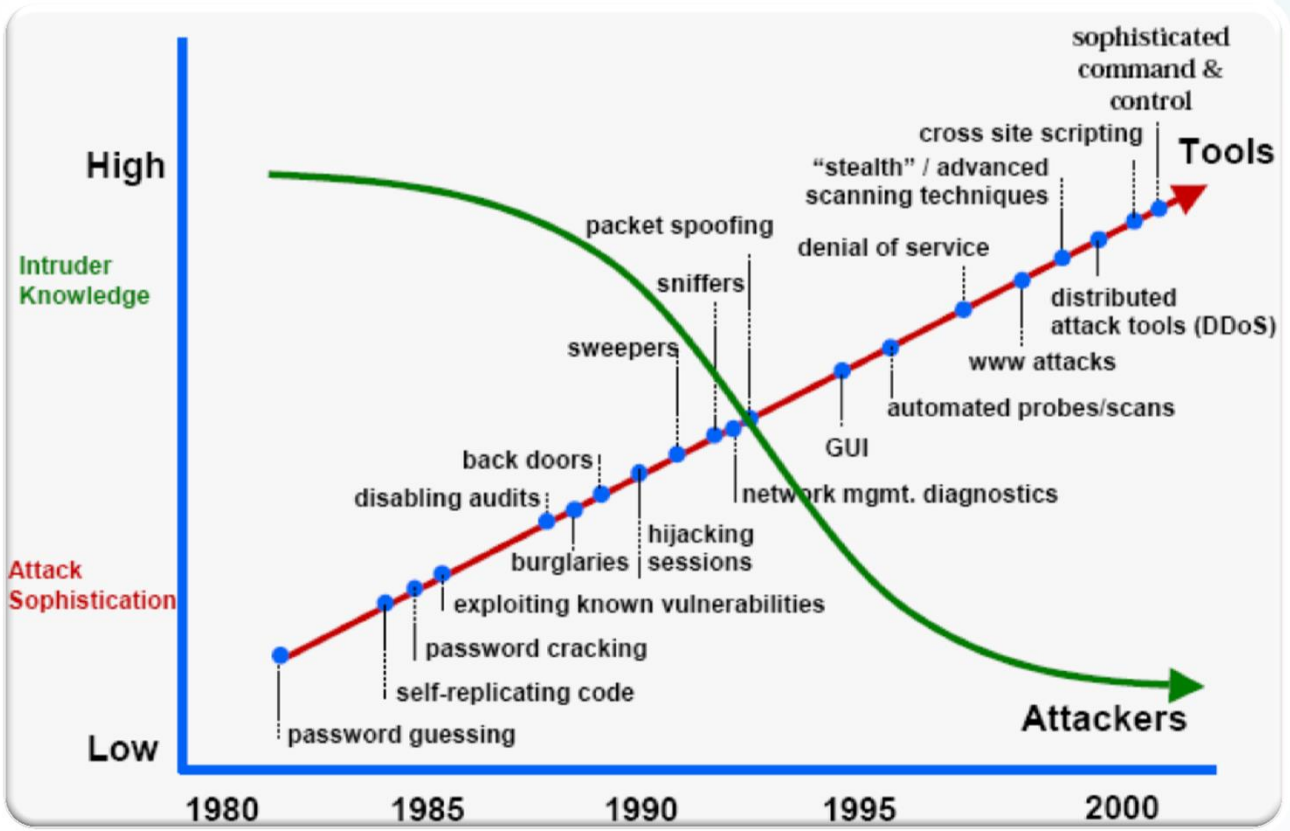


Evolução da SegInfo



(Hitchcock, 2005)

Evolução da SegInfo



Fonte: H.F. Lipson, CERT Coordination Center, CMU/SEI-2002-SR-009

Evolução da SegInfo

- Massificação das TIC (*E-everything*)
- Novas ameaças: Violação dos direitos de cópia, pornografia infantil, fraude, roubo de identidade, *Distributed Denial of Service* (DDoS), … "*cibercrime*"
- Défice de regulamentação nas Engenharias ligadas às TICs
- Centros de emergência e coordenação (e.g., CERT-CC)
- Necessidade de políticas de segurança, educação e treino; normas e códigos de boas práticas
- Novas profissões e formações => Procura de um CBK (*Common Body of Knowledge*)

Currículo para SegInfo

- Visão governamental e empresarial

NIST 800-16	ISC² – domínios do CBK
Organização e Segurança de TICs	Segurança da Informação e Gestão do Risco
Gestão do risco	Arquitectura e Modelos de Segurança
Controlos operacionais	"Controlos operacionais"
Controlos técnicos	Controlo de Acesso
	Segurança no desenvolvimento de aplicações
Aquisição/Desenvolvimento de controlos	Segurança Física
Instalação/Implementação de controlos	Criptografia
Interligação de sistemas e partilha de informação	Segurança em telecomunicações e redes de dados
	Recuperação de desastres (BCP)
Legislação e regulamentação	Legislação, investigação e ética

Currículo para SegInfo

- Visão académica

Áreas	Sub-áreas
Gestão, Políticas e Resposta	Políticas de segurança (gerais e específicas de utilização e gestão de tecnologias de informação); Cultura de segurança (incluindo questões sociais e psicológicas); Privacidade; Protecção da propriedade intelectual; Normas; Responsabilidades de gestão e culpabilidade; Avaliação e gestão do risco; Resposta e recuperação de incidentes
Sistemas de Computação Seguros	Controlo de acesso (identificação, autenticação e autorização); Desenvolvimento de sistemas seguros; Avaliação; Bases de Dados e suas aplicações; Desenvolvimento de software; Auditoria; Operações de manutenção
Segurança em Redes	Redes, serviços e protocolos; Vulnerabilidades; Ataques; Gestão, monitorização, auditoria e análise forense; Infra-estruturas; Redes sem fios; Filtragem
Criptografia	Princípios fundamentais; Algoritmos simétricos e assimétricos; Protocolos criptográficos; Dispositivos de hardware; Assinatura digital; PKI; Aplicações da criptografia; Steganography

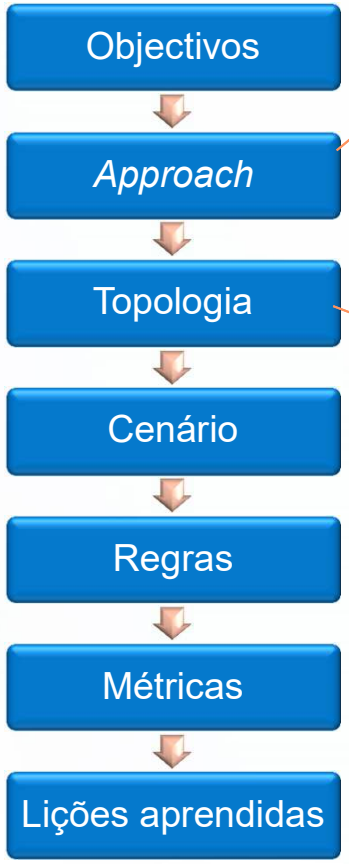
Currículo para SegInfo

- …identifica 7 áreas curriculares …

Area	Topics
Access Control and Privacy	Identification, authentication, authorization, anonymity and privacy
Risks and Attacks	Attacks, vulnerabilities, risks, intrusion detection, malicious software, testing and auditing, resilience
Cryptography	Applied cryptography, digital signature and digital certificates, key management and Public Key Infrastructures (PKI)
Network Security	Fundamentals of computer networks, communication protocols and security algorithms, and firewalls
Computer Security	Software vulnerabilities, OS security, malicious software
Business Continuity	Business continuity planning
Ethics and Legislation	Legal and ethic issues

Atividades pedagógicas

- *Cyber Defense Exercise* (CDX)



- Orientado aos ataques
- Orientado à defesa
- Híbrido

- Defensor
- Sistema alvo
- Infra-estrutura
- Atacante

(Patriciu, 2009)