PCS-2055, PCS-2582
Segurança da Informação

Serviços, Modelos e Políticas de Segurança

Bibliografia

- William Stallings, “Cryptography and Network Security - Principles and Practice”, 4th Edition, Prentice Hall, 2006.
- Douglas R. Stinson, “Cryptography - Theory and Practice”, 3rd Edition, CRC Press, 2005.
- Alfred Menezes, Paulo C. van Oorschot, Scott Vanstone, “Handbook of Applied Cryptography” CRC Press, 1997.

Motivação para a Segurança

Economia na Internet

- Cenário prévio: redes privativas, soluções proprietárias e recursos individualizados (acesso controlado, mas custo elevado).

- A integração de sistemas em larga escala contribuiu enormemente para a *redução de custos* devido ao *compartilhamento de recursos computacionais* e à adoção de *padrões abertos de comunicação*.

Economia na Internet

- Os dados a seguir são baseados num estudo da empresa de consultoria Booz-Allen & Hamilton.
- Definiu-se para esse estudo uma unidade de custo de transação financeira que leva em conta todos os custos envolvidos na transação.
- Consideraram-se as seguintes opções de estrutura de sistema:
  - Acesso via agência (sistema tradicional);
  - Acesso via rede telefônica (Home Banking);
  - Acesso via Internet (Internet Banking).

Custos por transação

- Agências US$ 1,08
- Home Banking US$ 0,54
- Internet Banking US$ 0,13

- O ganho observado pelo Internet banking é de quase uma ordem de grandeza (*10 vezes*) em relação ao custo das agências, e praticamente *5 vezes* em relação ao Home Banking tradicional (redes privadas).

O problema da segurança

- As informações que circulam na Internet:
  - passam por roteadores de terceiros;
  - percorrem caminhos diferentes a cada transação.
- ∴ Facilmente observáveis quando transitam pela rede.
- Enorme facilidade de acesso à Internet propicia que um grande número de usuários mal-intencionados (“hackers” e “crackers”) possa, em princípio, interferir negativamente num sistema transacional online.

O problema da segurança

- O *compartilhamento de recursos* de infra-estrutura que propicia o *ganho e economia de escala* é o mesmo fator que eleva a questão de *segurança ao primeiro plano* de preocupações para todos aqueles que planejam implantar um sistema online na Internet.

- *Como aproveitar a infra-estrutura de comunicação, beneficiando-se da redução de custos propiciada pelo compartilhamento de recursos, e ainda garantir a robustez de um sistema transacional?*

Serviços básicos da segurança

- Confidencialidade
- Integridade
- Legitimidade
  - Autenticidade
  - Irretratabilidade
- Disponibilidade

Confidencialidade

- Garantia de que qualquer informação armazenada num sistema de computação ou transmitida via rede seja revelada, acessada e/ou manipulada somente por usuários devidamente autorizados.

- Observação: *informação* ≠ *dado* (representação da informação).

- Um dado pode estar acessível a qualquer entidade e mesmo assim não revelar a informação aí contida.

Integridade

- Possibilidade de verificar a consistência da informação contida nos dados, impedindo que seja alterada indevidamente de maneira imperceptível.

- Detalhe: o serviço de integridade *não* garante que os dados não sejam alterados. A garantia efetiva é que, se os dados forem alterados sem autorização, a alteração será sempre *detectada*.

Legitimidade

- Garantia de que os recursos de um sistema não sejam utilizados por entidades não autorizadas ou de forma não autorizada.
  - *Autenticação*: a identidade alegada por um usuário é verificável e intransferível.
  - *Irretratabilidade*: nem o originador nem o destinatário das informações podem negar a sua transmissão, recepção ou posse.

Disponibilidade

- Garantia de que os usuários legítimos não sejam impedidos indevidamente de acessarem as informações e os recursos do sistema.

- Serviço essencialmente extra-criptográfico (físico), e o mais arquitetural/empírico/ heurístico dentre os serviços básicos da segurança.

Ameaças típicas

Ameaça	Descrição
Abuso	Uso para outra finalidade.
Recusa de serviço	Impedimento indevido de funcionalidade.
Espionagem	Obtenção ativa e indevida de informação.
Vazamento	Revelação passiva e indevida de informação.
Violação de integridade	Edição não autorizada de informação.
Personificação	Passar-se por outro.
Repetição	Retransmissão ilegítima.
Retratação	Negação falsa de uma ação ou informação.
Exaustão	Sobrecarga de utilização de recurso.
Porta dos fundos	Entrada indevida, oculta no sistema.
Cavalo de Tróia	Componente invisível mal intencionado.
...	...

Esta enumeração é útil para montar defesas ?

Mecanismos de Segurança

- Conjunto de:
  - Técnicas;
  - Procedimentos;
  - Algoritmos.

- Utilizados *adequadamente*, garantem a implementação dos serviços básicos de segurança de computação ou de comunicação.

Política de Segurança

- Conjunto de *regras e procedimentos* aplicáveis a *todas as atividades* relacionadas à segurança da informação dentro de um determinado *domínio*, sob a responsabilidade de uma *autoridade*.

- Domínio de Segurança:
  - Conjunto de recursos de comunicação e processamento de uma organização.

- Autoridade de segurança:
  - Entidade responsável pelo domínio de segurança do sistema de informação.

Política de Segurança

- Deve enumerar os *objetivos* a alcançar, os *requisitos* para atingi-los;
- Deve definir claramente as *autoridades*, *responsabilidades* e *auditorias* de segurança no âmbito do sistema.

Política de Segurança

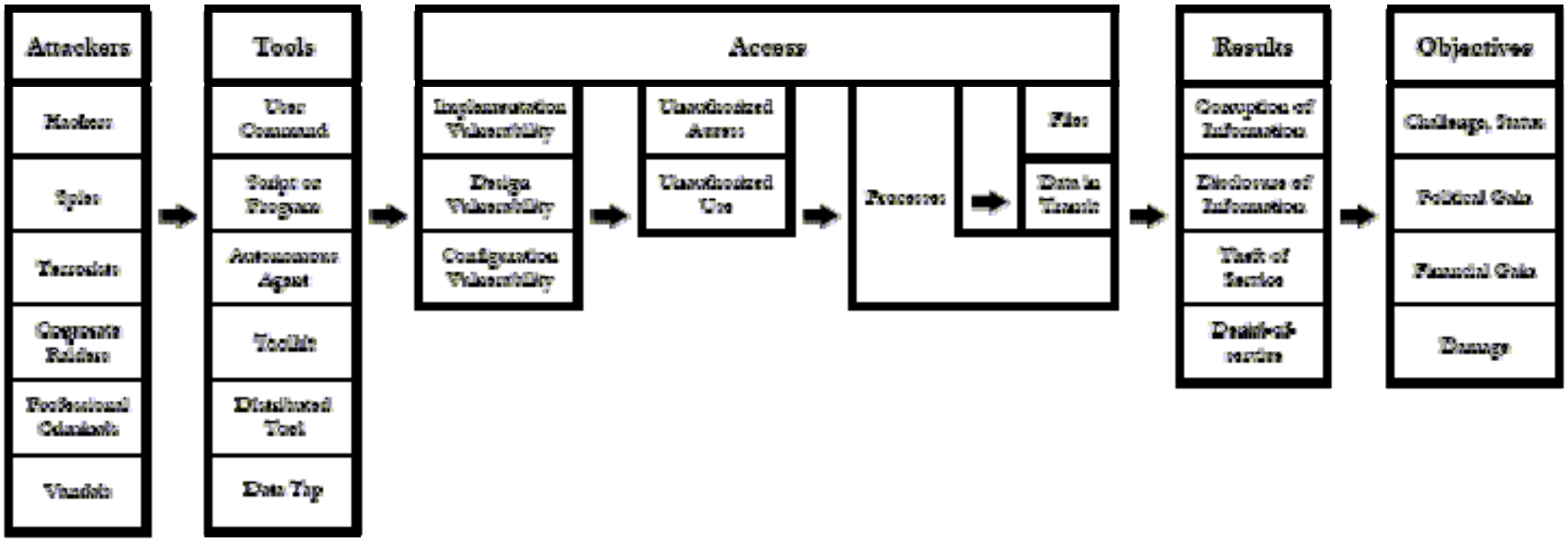
- Segurança é um ***processo***!
- Planejamento de implantação;
- Acompanhamento, avaliação e auditoria interna e externa periódica.

- ... A noção de segurança ainda precisa de uma definição formal capaz de orientar a confecção de políticas!

Segurança: Definição Formal

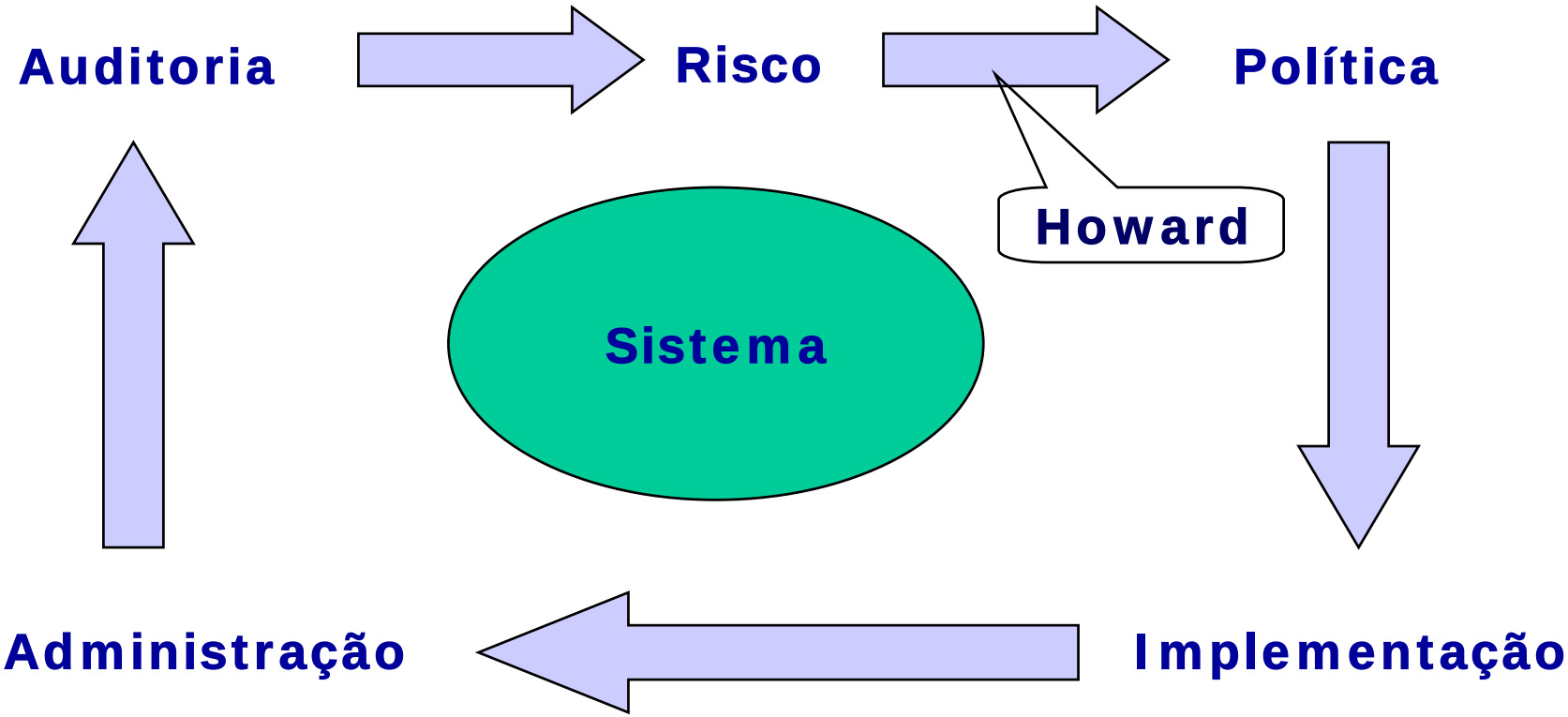
- “Computer security is preventing attackers from achieving objectives through unauthorized access or unauthorized use of computers and networks.” (Howard)

Taxonomia de Ataques



- Esta taxonomia, mesmo *incompleta*, pode nortear a elaboração de uma *política de segurança*.

Processo da Segurança



Computer vs. Network Security

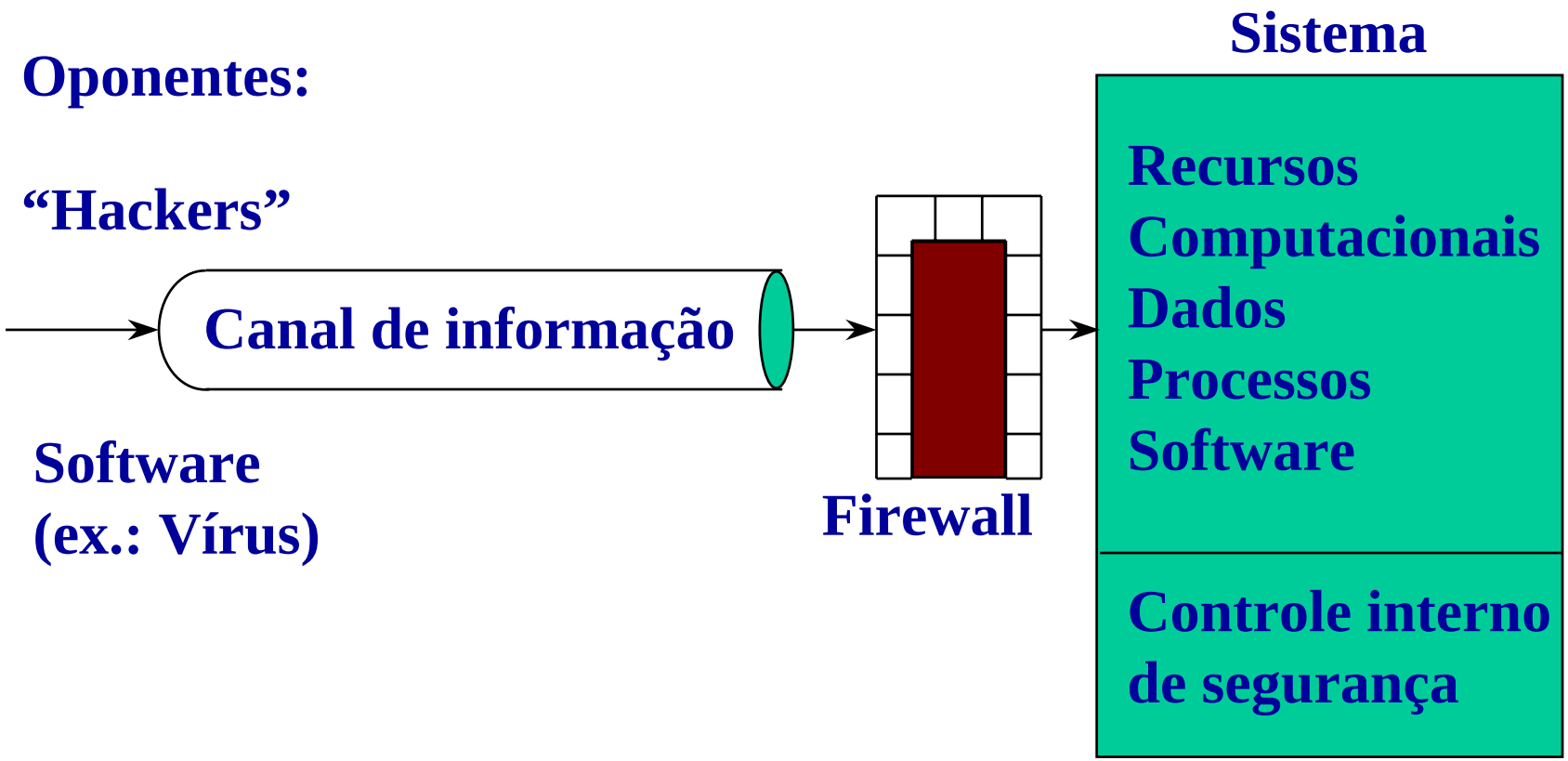
- “Computer Security”: técnicas e ferramentas que protegem um sistema de computação isolado.

- “Network Security”: técnicas e ferramentas que protegem um sistema de computação distribuído.

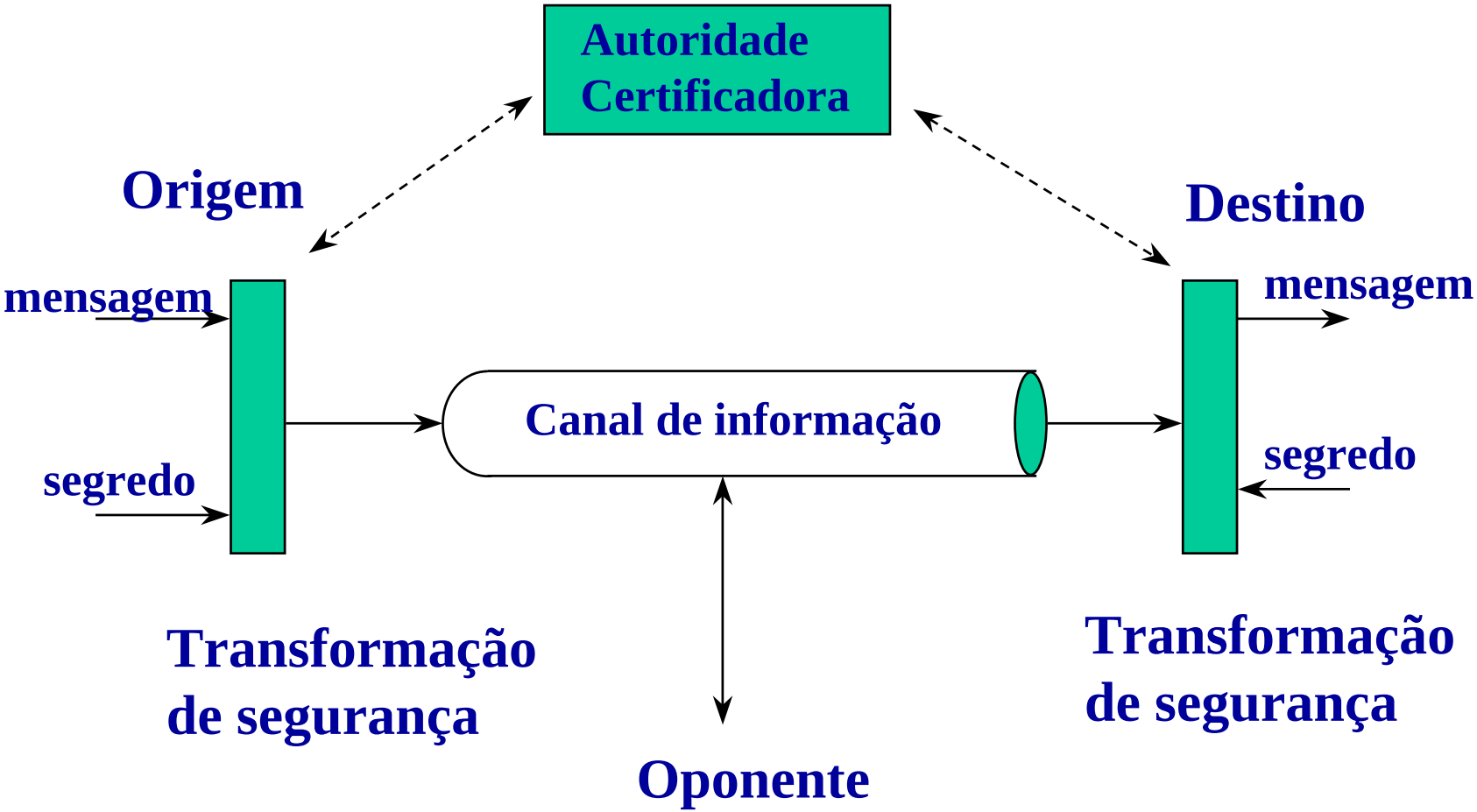
Computer vs. Network Security

- Não existe uma linha divisória muito clara entre “Computer Security” e “Network Security” (divisão geralmente de natureza didática).
- Os dois tipos são extremamente necessários e interdependentes – qualquer solução de segurança deve contemplar os dois aspectos com igualdade de importância.

Modelo para Computer Security



Modelo para Network Security



Engenharia de Segurança

- Soluções de segurança devem adequar-se ao cenário específico de cada sistema.
- Não existe panacéia: projeto deve atender as condições operacionais e os objetivos que se quer atingir.

Engenharia de Segurança

- Exemplo: Autenticação Digital (SEFAZ/SP).

- Sistema prévio (até 2000):
  - Autenticação mecânica de pagamentos (impressora autenticadora);
  - Liberação de documentos por operador (senha);
  - Fraudes!

Engenharia de Segurança

- Sistema desejado:
  - Processo automático, sem intervenção de operador (exceto digitação, se for o caso).
  - Comprovante impresso em 2 linhas de 32 colunas alfanuméricas (320 bits).
  - Fluxo de 2–4 milhões de autenticações mensais tratável com um único PC (Pentium 400 MHz).
  - Segurança de mercado (“RSA-1024”).
  - Especificação aberta, sem incidir em patentes.
- *Não existia tecnologia que atendesse a todos esses requisitos!*

Técnicas de Segurança

- Criptografia simétrica;
- Criptografia assimétrica;
- Algoritmos e protocolos auxiliares;
- Certificação digital e infra-estrutura de chaves públicas;
- Recursos extra-criptográficos:
  - Tokens e cartões;
  - Biometria.

Algoritmos Criptográficos

- Técnicas matemáticas de proteção de informações.
- Classificam-se conforme o tipo das informações compartilhadas entre o remetente e o destinatários de uma mensagem.

Simétricos	Assimétricos	Auxiliares
A segurança depende da posse de uma ***informação secreta*** comum ao remetente e ao destinatário, mas desconhecida por adversários.	A segurança depende da posse de uma ***informação confiável*** comum ao remetente e ao destinatário, potencialmente conhecida também por adversários.	A segurança ***independe*** de informação comum, ou depende de um ***segredo particular*** do remetente.

Análise de Segurança

- Dois critérios de segurança de algoritmos:
  - ***intrínseca*** (resistência do algoritmo em si diante de criptoanálise);
  - ***extrínseca*** (efeito do algoritmo no contexto e ambiente de um sistema).

- Algoritmos fortes combinados de maneira imprópria podem resultar em sistemas *fracos*!

Escolha de Algoritmos

- Segurança integrada: combinação adequada de algoritmos (sem partes “soltas”).
- Eficiência:
  - Consumo de processamento e de energia;
  - Espaço de armazenamento de dados e código,
  - Utilização de banda em canais de comunicação.
- Funcionalidade (nem todos os algoritmos têm as mesmas propriedades).
- Flexibilidade e interoperabilidade.
- Obsolescência de padrões.

Criptoanálise

- A maneira usual de avaliar a segurança de um sistema é tentar atacá-lo.
- Criptoanálise: sistematização matemática de técnicas gerais de ataque.
  - Até 1990, ataques contra algoritmos criptográficos eram essencialmente *ad hoc*.
  - Conhecem-se hoje publicamente dezenas de abordagens.

Criptoanálise – Nomenclatura

- *Texto claro* (ou *legível*): mensagem ou informação cuja privacidade se deseja salvaguardar.

- *Texto cifrado* (ou *criptograma*): resultado de uma transformação inversível aplicada ao texto claro.

Criptoanálise – Nomenclatura

- Por informação disponível:
  - Ataque de texto cifrado puro.
  - Ataque de texto conhecido.
  - Ataque de texto escolhido (claro ou cifrado).
  - Ataque adaptativo de texto escolhido.
  - Ataque de chave relacionada.
- Por informação obtida:
  - Ataque de recuperação de chave.
  - Ataque de inversão global.