

KRYPTUS

CPS – Criptoprocessador Seguro
Proteção de Comunicações e Dados

Roberto Gallo <gallo@kryptus.com>
Diretor Executivo

Sobre a Empresa

- Fundada em 2003 por pesquisadores e ex-alunos da Unicamp
 - Oriunda do LSC-IC-Unicamp
- Desde 2005 projetou, desenvolveu e produziu mais de 10 produtos de hardware e 5 de software para aplicações de segurança da informação
 - Desde semicondutores até aplicativos
- Líder do mercado nacional em pesquisa e desenvolvimento de hardware seguro

Sobre a Empresa

- Orçamento para pesquisa e desenvolvimento em S.I. para os próximos 30 meses de R\$7 milhões.
- Líder do mercado nacional de Hardware Security Modules (HSMs)
 - Volume 2 vezes maior que a segunda colocada
- Primeiro CI criptográfico comercialmente disponível no Brasil
 - Acelerador AES semi-condutor
- Parcerias estratégicas de desenvolvimento com instituições diversas:
 - RNP, LC e /LSC-IC-Unicamp, CEPESC/PR

Cases

- Alguns clientes e usuários finais de soluções e serviços KRYPTUS
 - MRE, TSE, GSI, Sisbin, ICP-Brasil, Braskem, FITec, Lucent, CPqD, CEPESC/PR, Ministério da Defesa, RNP, ITI/PR, SERPRO, Receita Federal, Justiça, CTI/Cenpra, Abin, FINEP, ANSP/FAPESP, Unicamp, UFF, USP, UFSC, UFV, UFMS, UFMG...
- Empresa se consolidou como Laboratório fornecedor de tecnologia para centros de pesquisa e universidades

Portfólio :: Serviços

- Análise de segurança de soluções em hardware, firmware e software
 - Aspectos de arquitetura e implementação
 - Adequação com padrões:
 - (ICP-Brasil, FIPS 140-2, ISO 27000)
- Reengenharia de produtos de hardware, firmware e software
 - Para modernização/atualização tecnológica
 - Para adaptações de segurança
- Desenvolvimento completo (ou parcial) de produtos para segurança da informação, incluindo hardware, firmware e software
 - Da análise de requisitos à gerência de produção

Algumas Tecnologias Dominadas

- Produção de IP-Cores seguros para FPGAs/CPLDs Altera e Xilinx (VHDL)
- Produção de software seguro em ambientes Windows/Linux/FreeBSD (ASM, C, C++, Java)
 - Bibliotecas criptográficas (Curvas Elíptica, RSA, SHA-2, HMAC, AES...)
- Produção de firmware seguro para plataformas ARM, MSP, AVR, PIC, etc (ASM, C)
 - Bibliotecas criptográficas
- Desenvolvimento de sistemas com:
 - Múltiplos protocolos de I/O (USB, PCI, PCI-Express, SMB...)
 - Baixo consumo, resistência ambiental
 - Baixo custo, tolerância a falhas

Portfólio :: Produtos

- KRYPTUS ASI-HSM – Hardware Security Module
 - Geração e gestão de chaves ICP-Brasil (e NFe)
- Token Criptográfico KeyGuardian
 - Cifração de arquivos e uso de chaves ICP-Brasil
- CompactHSM – Hardware Security Module de baixo custo para aplicações de NFe
 - Especial para mercado de entrada
 - Preço mais competitivo do mercado
- KRY1066 – Primeiro CI (ASIC) AES nacional

Desenvolvimento de Hardware



Sumário da Subvenção FINEP

- Projeto Pesquisa, Desenvolvimento e Piloto de Criptoprocessador Seguro para Aplicações Críticas
- Produto principal:
 - Lote piloto de 200 a 2000 unidades funcionais
- Tempo total de execução do projeto: 30 meses
- Montante de R\$ 4.276.308,00
 - Terceiro maior orçamento na área de TI
 - Quinto maior orçamento global de pequena empresa
- Produto inovador em termos globais
 - Coloca o país em posição destaque

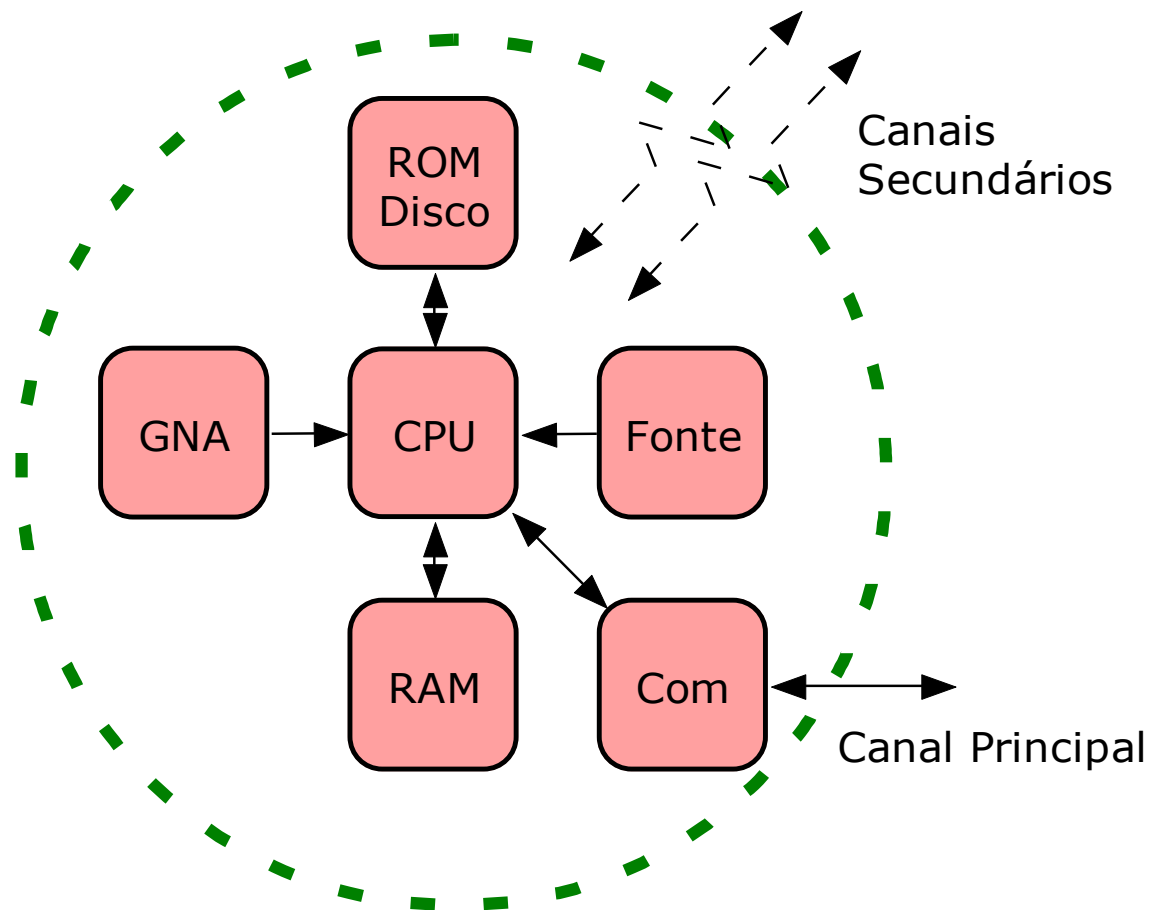
Sigilo das Comunicação e Conflitos

- 50 – Cesar já utilizava cifração de mensagens com valor militar
- 1941 - Quebra da Enigma foi fundamental na Batalha de Tenaro e diversas outras – Foi decisivo na 2ª Guerra
- 2008 - Infra-Estrutura de Comunicação desativada pelos Russos antes da Invasão da Georgia
- Criptoanálise militar é realidade em diversos países – NSA recentemente tornou público livros de 1938

Pontos de Ataque aos Sistemas Seguros de Comunicação e Dados

- Criptoanálise de algoritmos e protocolos
 - CM: Emprego de algoritmos e protocolos de Estado. Brasil tem competência (CEPESC/GSI)
- Exploração de canais secundários (cavalos de Troia em hardware, características de implementação – HW/FW/SW)
 - CM: Desenvolvimento 100% auditado
 - CM: Implementação SCA-aware
- Recuperação de chaves diretamente nos dispositivos
 - CM: Emprego de proteção de sistemas de sensoricamente e zeração (e. g. ASI-HSM)
 - CM: Cifração/autenticação de barramentos (mem)
- Adulteração de código executável

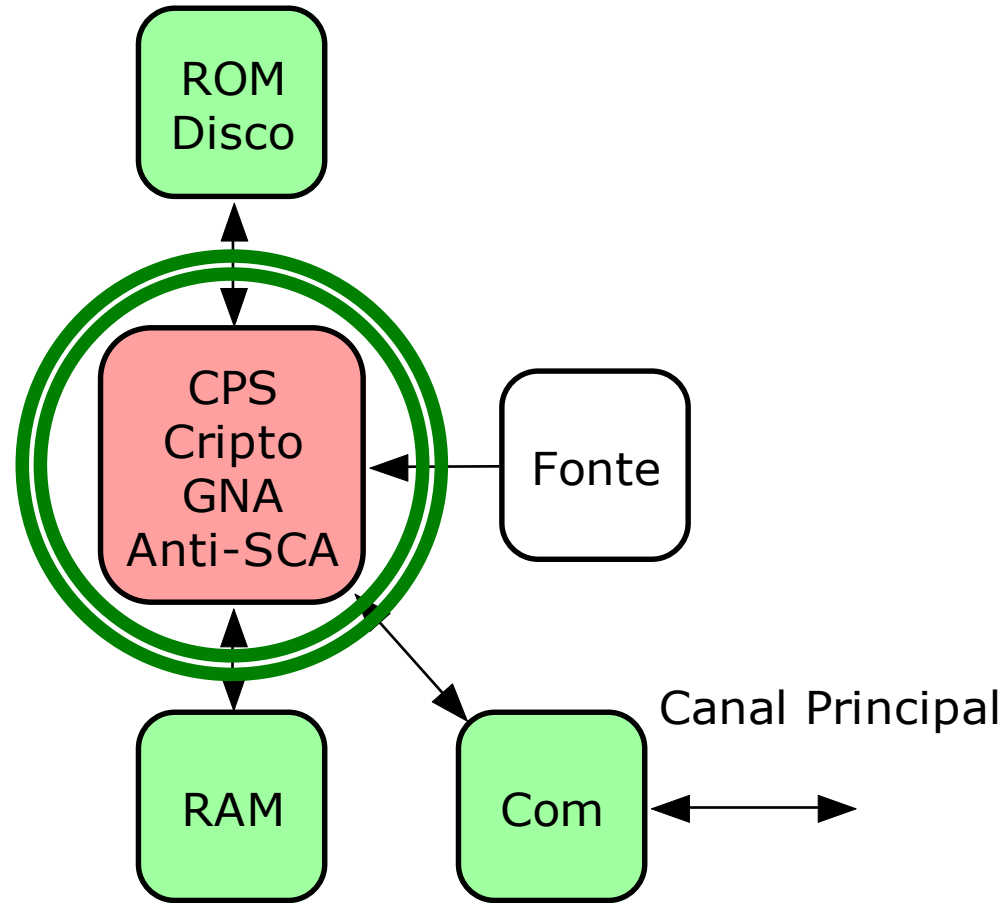
Fragilidades de Sistemas



Idéia Base do CPS

- Instanciação de núcleo uP de uso geral RISC 32 bits
 - SPARC, MIPS, ...
 - Código multi-aplicação (Linux Desktop)
- Cifração e autenticação total de memória em HW
 - Mem dados e programas (RAM, Disco, ...)
 - Algoritmos de Estado, padrões como AES, SHA-2
- Inspeccionabilidade total da arquitetura e código
 - VHDL (IP-cores) e software de todos componentes sob domínio nacional
- Gerador de números aleatórios on-chip
 - Qualidade do material de chaves criptográficas
- Guarda segura de chaves on-chip

Melhoria do Nível de Segurança



Benefícios

- Emprego em múltiplas aplicações
 - Rádios comunicadores (portáteis, para embarcações),
 - Cifradores de link (terrestres, rádio, satélite),
 - Execução segura de código (certificada, cifrada e assinada) em diversos ambientes,
 - Certificação digital (HSMs),
 - Votação eletrônica (Urna Eletrônica)

Benefícios II

- Dificultar criptoanálise
 - Emprego de Algoritmos de Estado
 - Dificuldade na extração dos Algs do hardware
- Eliminar chance de cavalos de Troia em hardware
 - Design inspecionável e sob controle nacional
- Minimizar ataques via canais secundários
 - Implementação de mecanismos anti-SCA

Futuro: Fase 2 do Projeto

- Deverá iniciar-se paralelamente à Fase 1
- Versão aeroespacial do processador, tolerante a falhas
 - Investimento e desenvolvimento no processador, sistema operacional e aplicações
 - Resistência a condições ambientais extremas
- Versão para smartcards do processador
 - Baixo custo, baixo consumo
 - Independência tecnológica em tecnologia chave



Obrigado
Roberto Gallo
gallo@kryptus.com